NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN INTEGRATIVE RISK MANAGEMENT/GOVERNANCE FRAMEWORK FOR HOMELAND SECURITY DECISION MAKING

by

Albert M. Ponenti

March 2008

Thesis Advisor: John Rollins
Second Reader: Lauren Wollman

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
March 2008

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE An Integrative Risk Management/Governance Framework for Homeland Security Decision Making

5. FUNDING NUMBERS

6. AUTHOR(S) Albert M. Ponenti

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

National leaders, federal legislation, and the Department of Homeland Security all endorse the adoption of a risk management framework as an application for homeland security decision makers. Risk Management Frameworks developed by the Department of Homeland Security (DHS), the Government Accountability Office (GAO), and the International Risk Governance Council (IRGC) contain the elements for building a robust risk management framework for homeland security decision-making. Yet no single framework is perfect or perfectly applicable to homeland security, mainly because of the uncertainty and complexity of terrorism. This leaves the decision-maker with a series of challenges, the most pressing of which is to manage risk in the ever evolving arena of homeland security.

This paper analyzes the principles of decision making and links them with the risk management processes illustrated in each of the frameworks. The final product is an integrative risk management/governance framework and an evaluation of its utility in a sample context: the nation's passenger rail system. This study narrows the focus even further by conducting a threat analysis on the passenger rail system for the New York and New Jersey region, and applying the integrative risk management/governance framework against a hypothetical terrorist threat on that system.

14. SUBJECT TERMS
Risk Management Framework, Risk Assessment, Decision Making, Risk Management/Governance, Homeland Security Problem Space, Uncertainty, Complexity, Passenger Rail Risk

15. NUMBER OF PAGES
143

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

AN INTEGRATIVE RISK MANAGEMENT/GOVERNANCE FRAMEWORK FOR HOMELAND SECURITY DECISION MAKING

Albert M. Ponenti
Sergeant First Class, New Jersey State Police
M.A., Seton Hall University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2008

Author: Albert M. Ponenti

Approved by: John Rollins, Ph.D.
Thesis Advisor

Lauren Wollman, Ph.D.
Second Reader

Harold Trinkunas, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

National leaders, federal legislation, and the Department of Homeland Security all endorse the adoption of a risk management framework as an application for homeland security decision makers. Risk Management Frameworks developed by the Department of Homeland Security (DHS), the Government Accountability Office (GAO), and the International Risk Governance Council (IRGC) contain the elements for building a robust risk management framework for homeland security decision making. Yet no single framework is perfect or perfectly applicable to homeland security, mainly because of the uncertainty and complexity of terrorism. This leaves the decision maker with a series of challenges, the most pressing of which is to manage risk in the ever-evolving arena of homeland security.

This paper analyzes the principles of decision making and links them with the risk management processes illustrated in each of the frameworks. The final product is an integrative risk management/governance framework and an evaluation of its utility in a sample context: the nation’s passenger rail system. This study narrows the focus even further by conducting a threat analysis on the passenger rail system for the New York and New Jersey region, and applying the integrative risk management/governance framework against a hypothetical terrorist threat on that system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CA	Consequence Analysis
CI/KR	Critical Infrastructure / Key Resources
COA	Course of Action
CRS	Congressional Research Service
DHS	Department of Homeland Security
DM	Decision Making
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
GEOINT	Geospatial Intelligence
HITRAC	Homeland Infrastructure Threat and Analysis Center
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IASNF	Identify Assets-Systems-Networks-Functions
IC	Intelligence Community
IED	Improvised Explosive Device
IRGC	International Risk Governance Council
JIC	Joint Intelligence Center
JTTF	Joint Terrorism Task Force
LEINT	Law Enforcement Intelligence
MA	Mission Areas
MASINT	Measurement and Signatures Intelligence
MDMP	Military Decision-Making Process
NADB	National Asset Database
NHC	National Hurricane Center
NIPP	National Infrastructure Protection Plan
NJSP	New Jersey State Police
NRC	Nuclear Regulatory Commission

NYPD	New York City Police Department
OSINT	Open-Source Intelligence
PAPD	Port Authority Police Department
PATH	Port Authority Trans-Hudson
PRP	Public Risk Perception
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RIC	Regional Intelligence Center
RISE	Regional Information Sharing Environment
ROIC	Regional Operations Intelligence Center
RPD	Recognition-Primed Decision Model
SIGINT	Signals Intelligence
SRA	Society for Risk Analysis
SSA	Sector-Specific Agency
SSP	Sector-Specific Plans
TC	Target Capabilities
TCL	Target Capabilities List
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
UTL	Universal Task List
VA	Vulnerability Assessment

ACKNOWLEDGEMENTS

I would like to thank the New Jersey State Police for allowing me to pursue educational opportunities, one of which has been attending the Naval Postgraduate School. I am especially thankful to Colonel Joseph Fuentes and the NJSP Command Staff. I express my deepest appreciation for your leadership, vision, and interest in my participation at NPS.

I also need to acknowledge the men and women of the Homeland Security Branch, who are committed to protecting the homeland, especially to my friends and colleagues of the T.E.A.M.S. Unit. Your unwavering dedication to duty and commitment to one another goes unnoticed. Thanks for being there.

I am also indebted to Captain Ed Cetnar, for his professionalism, friendship, and unending support for me attending the NPS. To Lieutenant Ray Guidetti, my colleague, friend, and NPS mentor. It would not have been possible to have experienced this insightful journey if you had not paved the way for me, as well as the many troopers to follow.

Although it is impractical to thank all of those who have been there for me over the past eighteen months, there are some who warrant special recognition. Dr. Chris Bellavita, thanks for allowing me to think strategically, not operationally. I would also like to thank my advisors: Dr. John Rollins, for his flexibility, insight and guidance, and Dr. Lauren Wollman, for her patience, and the one who convinced me that I understood the research, but just needed to write about it. To my classmates of 0603-0604, your friendships will last a lifetime. A special thanks to my pals, who liked to eat and enjoy the landscape of Monterey.

Moreover, I am forever thankful to my mother and father, who have defined resiliency and sacrifice throughout my lifetime. You have provided me with the spirit and opportunity to always shoot for the stars. Thanks for your unending love and guidance.

Finally, I am grateful for the sacrifices endured by my wife Bonnie, son Michael, and daughter Angelina. You guys have inspired and supported me from day one. Your encouragement and love is priceless. I owe you all.

I. INTRODUCTION

A. PROBLEM STATEMENT

Managing homeland security risk, which can stem from both terrorism and natural disaster, is an enormously complex undertaking and is also a critical task, considering the need to deploy finite resources effectively. During his testimony before the Homeland Security Subcommittee of the Senate Appropriations Committee, Secretary Michael Chertoff addressed the importance of adopting a risk-management strategy toward homeland security preparedness:

> What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.[1]

As described by Secretary Chertoff, "threat, vulnerability, and consequence" are the guiding variables for managing risk. Yet, this is but one element of the risk-management process laid out by Secretary Chertoff. It is worth peeling back layers of the onion a bit further to explore the complexity of risk management framework applications that can assist the homeland security decision-making process.

Secretary Chertoff has called for the full adoption of a risk management framework. It is essential for the Department of Homeland Security (DHS) to assess risk by determining which elements of risk should be addressed and in what ways, within available resources. A risk management framework can assist decision makers in developing courses of action (COA) relative to the homeland security problem space. Fully integrating a risk management approach into decision-making processes is challenging for any organization, and is particularly challenging for DHS, with its diverse

[1] DHS Secretary Michael Chertoff in an April 20, 2005, Speech before the Homeland Security Subcommittee of the Senate Appropriations Committee, outlined a strategy for "risk management." http://www.dhs.gov/xnews/testimony/testimony_0035.shtm (Accessed on November 1, 2006).

set of responsibilities. The basic goal, however, across DHS homeland security programs, is similar: to identify, prevent where possible, and protect the nation from all risks to people, property, and the economy.[2] At the national level, this is a complex and critical undertaking. At the state and local level, it is even more complex, because governing bodies also have to deal with the additional priorities that stem from and are characteristic of regional constructs, social complexity, politics, economic factors, and infrastructure.

A comprehensive risk management framework can assist state and local leaders with homeland security decision making. Frameworks developed by the DHS *(Contained in the National Infrastructure Plan — NIPP)*, the Government Accountability Office (GAO), and the International Risk Governance Council (IRGC) contain the essential components and relative elements for building a robust risk management framework.

Each one of these risk management frameworks can assist the decision maker with resource allocation and situational, course-of-action decisions. No single framework is perfect or perfectly applicable to homeland security, however, mainly because of the uncertainty and complexity of terrorism. This leaves the decision maker with a series of challenges, the most pressing of which is to manage risk in the ever-evolving arena of homeland security.

B. HYPOTHESIS

The various frameworks utilized for this study illustrate a process for managing risk. If the core components and elements from each are extracted and integrated into a single, cohesive risk management/governance structure, will it effectively improve the decision-making process?

An important aspect of this study involves linking the elements of decision making with the risk-management processes illustrated in each of the frameworks. This will be accomplished by analyzing each of the components and their core elements, and

[2] United States Government Accountability Office, Homeland Security, *Applying Risk Management Principles to Guide Federal Investments,* GAO-07-386T (Washington, DC: February 7, 2007).

assessing their utility for the decision maker. Based on this analysis, we will be able to ascertain if the frameworks provide a logical set of actions that can produce a methodology for decision makers to follow.

The final objective will be to construct an integrative risk management/governance framework from the appropriate components of each of the frameworks, and evaluate its utility against an issue in the field of homeland security – that of the vulnerability of the nation's passenger rail system. This study will narrow the focus even further by conducting a threat analysis on the passenger rail system for the New York and New Jersey region, and applying the integrative risk management/governance framework against a hypothetical terrorist threat on that system.

The consumers of this research will be state homeland security decision makers who are in need of a risk management framework that can guide and assist with resource allocation and course-of-action decisions. This risk management/governance framework will provide an effective model.

C. LITERATURE REVIEW

The management of risk is important to industry, the economy, health and health care, and many other elements of society. Risk management and how it pertains to homeland security is a critical topic and a priority for the nation's homeland security mission.

What is truly the most efficient way to manage risk? According to Chertoff, addressing homeland security requires a risk-management strategy based on "the strategic matrix of threat, vulnerability, and consequence." Chertoff has stated that DHS must concentrate first on threats that could ultimately have catastrophic consequences.[3] This provides a basic framework from which to start, but requires a more in-depth look at risk management, the homeland security mission of state and local public safety responders, and how decisions regarding threats and/or terrorist attacks are made.

[3] DHS Secretary Michael Chertoff, U.S. Department of Homeland Security Second Stage Review, speech was conducted at the Ronald Regan Building, Washington, DC, July 13, 2005. http://www.dhs.gov/xnews/speeches/speech_0255.shtm (Accessed February 5, 2007).

A multitude of literature is available regarding what constitutes risk. Some authors distinguish between risk assessment and risk management, others do not. Some incorporate risk assessment within the broader risk management label. Yacov V. Haimes, in *Risk Modeling, Assessment, and Management,* makes the distinction between the two terms, while also recognizing significant overlaps.[4] Haimes explains that five steps constitute the entire risk-assessment and management process:

1. Risk identification
2. Risk modeling, quantification, and measurement
3. Risk evaluation
4. Risk acceptance and avoidance
5. Risk management

Haimes supports the use of models for decision makers, saying that models, methodologies, and procedures for risk assessment provide an essential service to decision makers — that of processing of data into intelligence — so the elements of risk that are associated with policy decisions can be properly valued, evaluated, and considered in the decision-making process.[5]

The National Preparedness Goal adopts a risk-based all-hazards approach that involves reorienting preparedness activities to enable officials to make informed choices that best manage risk and reduce impact. Risk is the product of threat, vulnerability, consequence, and likelihood of occurrence.[6] The National Preparedness Goal supports Secretary Chertoff's belief in a risk-based approach to homeland security. It also provides a capabilities-based strategy for managing risk, and references three capabilities-based planning tools: (1) The National Planning Scenarios; (2) The Universal Task List (UTL); and (3) The Target Capabilities List (TCL). With this approach, risk-based target levels can be customized for each capability and geographic area across the nation.[7] The

[4] Yacov V. Haimes, *Risk Modeling, Assessment, and Management*, 2nd ed. (John Willey & Sons, 2004), 56.

[5] Ibid., 59.

[6] Department of Homeland Security, *National Preparedness Goal,* 2005, 3.

[7] Ibid., 7.

National Preparedness Goal provides capabilities that can assist in reducing risk, yet it does not provide a model for where these capabilities fit into the risk equation for threat, vulnerability, and consequence.

A GAO report titled *A Risk Management Approach Can Guide Preparedness Efforts*, identifies a risk management model that is inclusive of an assessment process. According to the report, risk management is a systematic and analytical process that allows the decision maker to determine whether, and to what degree, a threat or attack will endanger an asset (e.g., a structure, individual, or function). Risk management also facilitates the identification of actions that can reduce the risk and mitigate the consequences. The report states that an effective risk management approach includes a threat assessment, a vulnerability assessment, and a criticality assessment. A threat assessment identifies and evaluates threats based on various factors, including capability and intention, as well as the potential impact. Vulnerability assessments and criticality assessments complete the equation, and allow the decision maker to better prepare against threats.[8] The report does not delineate which processes are involved with conducting the various assessments, but it does conclude that a risk management strategy will drive the preparedness effort as it pertains to homeland security.

Robert G. Ross, chief of the Risk Sciences Branch of DHS, takes a step back and provides a more philosophical and big-picture discussion of risk and its consideration in homeland security decision making. In *Risk and Decision-Making in Homeland Security*, Ross examines the decision-making process and the complex, adaptive systems that are endemic to the nation's terrorist adversaries.[9] Ross argues that the risk assessment framework currently used by DHS is inadequate and far from being understood. His paper identifies various models that are associated with risk management, and outlines the characteristics of a future DHS Risk Assessment "Tool Kit."

[8] General Accountability Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (October 31, 2001), 3.

[9] Robert G. Ross, "Risk and Decision Making in Homeland Security," Office of Comparative Studies, Department of Homeland Security Science and Technology Directorate (July 31, 2006).

A Congressional Research Service (CRS) Report for Congress, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, explains that terrorism risk analysis and assessment do not exist in a vacuum. Risk is analyzed and assessed as a means to mitigate or "buy down" risk over time by developing certain capabilities across the country. The State Homeland Security Grant Program is the primary tool used by DHS to do this. DHS has been very clear in utilizing a risk model for disseminating grant funds. These funds have helped state and local partners take the kind of action that not only reduce the risk of a terrorist attack, but also enable state and local agencies to respond effectively.[10]

The CRS Report presents several risk-assessment and related grant program options for congressional consideration. The report is broken down into three core areas: the Evolution of the DHS Risk Assessment Methodology; the Risk Assessment Stages of Development and Current Process; and Possible Approaches for Congress. The report includes risk management as a component of risk analysis, which it broadly defines as risk assessment, risk characterization, risk communication, risk management, and policy relating to risk in the context of risks that concern individuals, public and private sector organizations, and society at the local, regional, national, or global level. According to the CRS Report, risk analysis seeks to inform, not to dictate, the complex and difficult choices among possible measures to mitigate risk.[11]

D. REVIEW OF RISK MANAGEMENT FRAMEWORKS

One of the most comprehensive risk management frameworks is the International Risk Governance Council (IRGC) framework, which delineates the process into three primary Risk Governance Phases: Pre-Assessment, Risk Appraisal, and Risk Management. These categories are further delineated and associated with a certain product or process. An example of this would be the Pre-Assessment Phase. A core

[10] Todd Masse, Siobhan O'Neil, John Rollins, "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress," Congressional Research Service Report for Congress (CRS Order Code RL33858), February 2, 2007, 2. https://www.hsdl.org/homesec/docs/crs/nps .pdf [Accessed February 2007].

[11] Ibid., 16.

element of this phase is Early Warning and Monitoring. Early Warning and Monitoring are processes used to detect and/or neutralize a threat. The IRGC framework suggests that appropriate measures taken in the Early Warning and Monitoring stages can assist in reducing the threat. Threat in this sense, would be the likelihood that a particular asset, system, or network will suffer an attack or incident.[12] Associated Early Warning and Monitoring functions such as, Fusion Centers and Intelligence Dissemination tools can assist in reducing the threat.

Risk Characterization and Risk Evaluation are situated between Risk Appraisal and Risk Management, and can be assigned either to those charged with the assessment or those responsible for management, whichever is better equipped to perform the associated tasks. The IRGC framework also has Risk Communication as a companion to all phases of addressing and handling risk. However, the clear sequence of phases and steps offered by this process is primarily a logical and functional one, and will not always correspond to reality due to uncertainty and complex problems associated with risk.[13] Although the IRGC framework offers a very complex, integrative approach to fusing risk assessment and risk management under the umbrella of governance, it is a model that has yet to be utilized within the security studies domain.

In a GAO report released in 2007, risk management is recognized as a strategy for helping policy-makers make decisions about assessing risk, allocating resources, and taking actions under conditions of uncertainty.[14] To provide a basis for examining efforts for carrying out risk management, GAO developed a framework based on best practices and other criteria. The framework is divided into five phases: (1) Setting strategic goals and objectives, and determining constraint; (2) Assessing the risks; (3) Evaluating alternatives for addressing those risks; (4) Selecting appropriate alternatives; and (5) Implementing the alternatives and monitoring the progress made and the results

[12] Department of Homeland Security, *National Infrastructure Protection Plan,* 2006, 35.

[13] Ortwin Renn, International Risk Governance Council, “White Paper on Risk Governance: Towards an Integrative Framework,” September 2005.

[14] General Accountability Office, *Homeland Security: Applying Risk Management Principles to Guide Federal Investments*, GAO-07-386T (February 7, 2007), 3.

achieved.[15] The GAO report explains that the framework has been used to examine various programs, and that it will likely evolve as processes mature and lessons are learned. The disadvantage of the GAO framework is that its components are simplistic and offer very little guidance by way of inserting core elements that define how the framework can assist with the decision making process.

The cornerstone of the National Infrastructure Protection Plan (NIPP) is its risk management framework. The NIPP defines risk as the combination of the frequency of occurrence, vulnerability, and the consequence of a specific hazardous event. In the context of the NIPP, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.[16] The NIPP risk management framework establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector specific risk. It includes the following activities that can assist with the decision-making process: (1) Set security goals; (2) Identify assets, systems, networks, and functions; (3) Assess risk; (4) Prioritize; (5) Implement protective programs; (6) Measure effectiveness. The NIPP framework inserts core elements for each component of the structure, enabling the decision maker to make better informed decisions.

The literature and the briefly defined risk management models examined thus far have focused primarily on the elements of risk, and how they pertain to a particular framework or methodology. An essential component, however, is to integrate the risk management frameworks with decision-making processes. The Military Decision-Making Process (MDMP) is a planning model that establishes procedures for analyzing a mission, developing, analyzing and comparing courses of action against criteria of success and against one another, selecting the optimum course of action, and producing a plan or

[15] General Accountability Office, *Homeland Security,* 9.

[16] Department of Homeland Security, *National Infrastructure Protection Plan,* 2006, 29.

order. The MDMP applies across the spectrum of conflict and the range of military operations.[17] It is a model that can be utilized to drive the risk management framework at various levels.

Due to the ambiguity and uncertainty of risk and the possibility of an immediate threat surfacing, the decision-making process may need to be intuitive rather than the step-by-step process as defined by the MDMP. A Recognition-Primed Decision (RPD) model fuses two processes: the way decision makers size up the situation to determine whether a course of action makes sense; and mentally simulating, or imagining, the course of action to identify the possible consequences.[18] A comprehensive risk management framework can benefit from the RPD model, and assist in addressing elements of risk.

E. RESEARCH METHODOLOGIES

The GAO, NIPP, and IRGC frameworks illustrate the risk management process. Within each of the frameworks are the core components that drive the process. The methodology for this analysis will be to provide an overview of the frameworks' components, and ascertain how those components factor into the decision-making process. For each component, the decision-making processes discussed in the literature will provide the construct for the analysis. In addition, the elements that support each component will be linked to the various decision-making processes, with examples provided to show its relevance.

Based on this analysis, we will ascertain whether the frameworks provide a logical set of actions that a decision maker can follow. The commonalities extracted from each framework that prove to be effective will be identified and integrated into a risk management/governance framework. The final objective will be to generate an

[17] U.S. Department of the Army, "Army Planning and Orders Production," *Field Manual* 5-0: Washington, DC, January 20, 2005, 3-1.

[18] Gary Klein, *Sources of Power: How People Make Decisions*, Cambridge, Massachusetts: MIT Press, 1998, 24.

integrative risk management/governance framework built from the extracted components of each of the frameworks, and an evaluation of its utility against an issue within the homeland security arena.

For the purposes of this research, we will look at the qualitative principles associated with risk management, and stand clear of any quantitative analysis that would influence the use of statistical data, or risk allocation grant methodology. We will also look at the qualitative attributes of risk analysis and risk assessment principles, and how they support the risk management process. The problem space associated with risk and homeland security decision making is vast and dense. In order to appropriately assess the integrative risk management/governance framework, we will focus on the threat of terrorism, rather than natural and technological hazards.

Finally, through the principles associated with risk analysis and risk assessment, a qualitative threat analysis will be conducted for the passenger rail transportation system in the New York/New Jersey region. As was witnessed in the 2004 Madrid train bombings and the 2005 London bombings, the passenger rail transportation sector is a vulnerable target for terrorist organizations. We will create a threat-based scenario that targets the rail system in the New York/New Jersey region, and apply the integrative risk management/governance framework to it.

II. BACKGROUND

A. OVERVIEW OF TERRORISM RISK AND RISK CONCEPTS

1. Introduction

Part A of this chapter is intended to establish an acceptable and usable definition of terrorism risk, and to review some of the concepts and terminology that are utilized in risk management. For the purposes of this research, we will look at the qualitative principles associated with risk management, but will not undertake any quantitative analysis that would influence the utility of statistical data or risk allocation grant methodology. We will also look at the qualitative attributes of risk analysis and risk assessment principles, and how they support the risk management process. Finally, we will outline the methodology and foundation of risk analysis and risk assessment.

2. An Acceptable Understanding of Terrorism Risk

Robert G. Ross, in his paper "Risk and Decision Making in Homeland Security," includes seventeen definitions of risk — a list he acknowledges is by no means exhaustive. Each definition, however, was developed to illustrate a particular aspect of risk and its utility within the context for which it was developed. The reason risk can have so many different meanings, with each being right, Ross points out, is that risk, no matter how well-grounded in reality, is a mental and emotional construct rather than a physical reality.[19]

The Oxford English Dictionary defines risk is a "hazard, chance of, or bad consequences, loss."[20] Two elements emerge from this definition: the nature of the consequences of actions, and the likelihood of negative consequences.

[19] Robert Ross, "Risk and Decision Making in Homeland Security," 3.

[20] Zur Shapira, *Risk Taking: A Managerial Perspective* (New York: Russell Sage Foundation, 1994), 3.

The word “risk” is derived from the early Italian *risicare*, which means “to dare.” Peter L. Bernstein explains that risk is a choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about.[21]

The Nuclear Regulatory Commission (NRC) Glossary provides a less complex definition for risk, yet it captures its core meaning: Risk is the combination of (1) What can go wrong? (2) How likely is it? (3) What are the consequences?[22] Rather than analyze multiple definitions and the construct in which risk is utilized, this paper will focus on how risk and risk management apply to the domain of homeland security.

According to Yacov Y. Haimes, “To manage risk, one must measure it with appropriate metrics.” Haimes points out that this principle is applicable when addressing risks of terrorism; the first step is to identify all conceivable sources of risk. Haimes breaks it down into four major categories:[23]

1. Risk to human lives and to individual property, liberty, and freedom;
2. Risk to organizational-societal infrastructures and the continuity of government; operations, including the military and intelligence-gathering infrastructure;
3. Risk to critical cyber or physical infrastructures;
4. Risk to economic sectors.

Haimes writes that this is the first step in a decision-making process that will enable effective strategic and tactical planning. Although these categories are necessary, they are quite general, and would have a cascading impact on one another if a significant act of terrorism were to occur. However, the utility of these categories can be found if one narrows them down in terms of: (1) Who is targeting the U.S.? (2) What is going to

[21] Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York: John Wiley & Sons, 1996), 8.

[22] U.S. Nuclear Regulatory Commission: Full text Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html [Accessed January 28, 2008].

[23] Yacov V. Haimes, Risk Modeling, Assessment and Management, 685.

be targeted? (3) What will the consequences be? An example would be a homegrown, radicalized terrorist group executing an attack on a passenger rail transportation system, resulting in multiple casualties.

Department of Homeland Security (DHS) Secretary Michael Chertoff advocates a risk-based approach to homeland security. According to Chertoff, "DHS must base its work on priorities driven by risk and, increasingly, risk assessment and subsequent risk mitigation have influenced all of the department's efforts intended to enhance our nation's ability to prevent, respond to, and recover from future terrorist attacks and natural disasters."[24] Under Chertoff's direction, DHS manages risk in terms of threat, vulnerability, and consequence. DHS prioritizes policies and operational missions according to a risk-based approach, and has established a series of preventive and protective steps to increase security at multiple levels.[25]

Risk as an underlying principle has also been influential in the way DHS allocates grant funds. Using its risk assessment formula, DHS considers the threat (T) to a target/area, multiplied by vulnerability (V) of the target/area, multiplied by consequence (C) of an attack on the target area. As a result, the risk assessment formula is R=T*V*C.[26]

Henry Willis et al., of the RAND Corporation, view terrorism risk as having three components: the threat to a target, the target's vulnerability, and the consequences of a successful attack. People and organizations represent threats when they have the intent and/or the capability to damage a target. The threat to a target can be measured as the probability that the target would be attacked in a specific way during a specified period. Vulnerability is measured as the probability that damage would occur given a specific

[24] Masse et al., "The Department of Homeland Security's Risk."

[25] U.S. Department of Homeland Security, "Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security," Press Release, July 13, 2005, Office of the Press Secretary. http://www.dhs.gov/xnews/releases/press_release_0703.shtm. [Accessed on January 30, 2008].

[26] Masse et al., "The Department of Homeland Security's Risk."

threat. Consequences are the magnitude and the type of damage that would result from a successful terrorist attack. Risk is the function of all three components: threat, vulnerability, and consequences.[27]

By combining the categorical definitions of terrorism risk described by Haimes and the risk components of threat, vulnerability, and consequences as described by Secretary Chertoff and Willis et al., we can develop a model that places threat, vulnerability, and consequence, plus intent and capability (an element of threat) at the center; risk is placed on the periphery (see Figure 1).[28] This illustrates a broader definition of terrorism risk, and acknowledges that threat, vulnerability, and consequences are core components of risk analysis and management. For the purposes of this research, we will refer to this model as an acceptable definition of terrorism risk.

[27] Henry Willis et al., *Estimating Terrorism Risk* (Santa Monica, CA: RAND Center for Risk Management Policy, 2005), xvi.

[28] Figure 1 is meant to illustrate the link between risk and the elements of threat, vulnerability, and consequence. Throughout this research, and in the contents of multiple homeland security documents and testimonies, these elements seem to be at the core of homeland security risk.

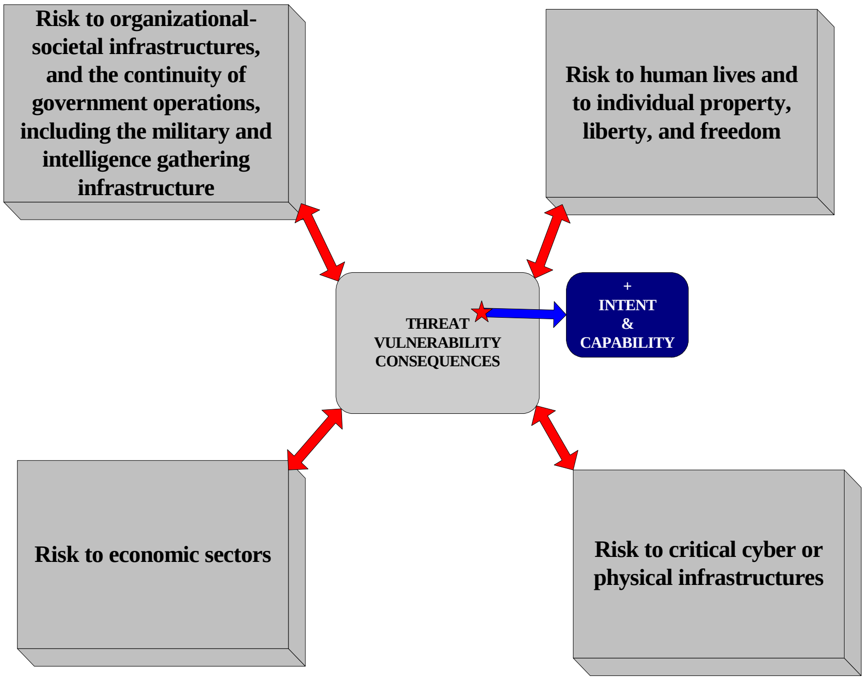

Risk to organizational-societal infrastructures, and the continuity of government operations, including the military and intelligence gathering infrastructure
Risk to human lives and to individual property, liberty, and freedom
THREAT
VULNERABILITY
CONSEQUENCES
+
INTENT
&
CAPABILITY
Risk to economic sectors
Risk to critical cyber or physical infrastructures

Figure 1. Broader Definition of Risk

3. Risk Concepts

One of the most significant challenges in addressing the concept of risk in any context is the absence of a commonly accepted lexicon and a set of professional practices, particularly as they relate to the relatively new field of homeland security risk.[29] Although this study focuses on the utility of risk management as it pertains to decision making, other terms related to risk are widely used. To ensure consistency and foster an understanding of where risk management fits into the "risk terminology" domain, it will be necessary to clarify risk concepts and definitions, and the utility they have for this paper.

According to Ross, there are several schools of thought on proper definitions and hierarchical relationship between the terms "risk assessment," "risk analysis," and "risk management." How each is defined and used often depends on who is leading the

[29] John P. Paczkowski, "Risk Management as Strategic Change in National Homeland Security Policy," Naval Postgraduate School Thesis, September 2007, 14.

discussion.[30] For example, the Society for Risk Analysis (SRA) uses the term "risk analysis" as its cornerstone phrase, whereas DHS uses "risk assessment" in most of its risk-formula terminology. The U.S. Coast Guard's Glossary of Risk Terms also provides definitions:[31]

> **Risk Analysis:** Used interchangeably with risk assessment.
>
> **Risk Assessment:** The overall process of identifying and analyzing risks. The process of characterizing hazards within risk areas by analyzing them for their potential mishap, consequences and probabilities of occurrence, and combining the two estimates to reach a risk rating.
>
> **Risk Management:** The process by which assessed risks are mitigated, minimized, or controlled through engineering, management, or operational means. This involves the optimal allocation of available resources in support of group goals.

A Congressional Research Service Report cites the SRA and its interpretation of risk analysis: Risk analysis is broadly defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risk concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level. Risk analysis seeks to inform, not to dictate, the complex and difficult choices among possible measures to mitigate risk.[32]

The International Risk Governance Council (IRGC) refers to risk analysis as a collective term that covers risk assessment, risk management, and risk communication.[33] Based on these two definitions, risk analysis seems to be the overarching term that captures both the assessment and management process. There are, of course, agencies and organizations that differ. For example, DHS differentiates between risk analysis and risk management, a philosophy that has been most evident in its resource allocation

[30]Robert Ross, "Risk and Decision Making in Homeland Security."

[31] United States Coast Guard's Glossary of Risk Terms, http://www.uscg.mil/hq/gm/risk/glossary.html [Accessed on March 18, 2008].

[32] Masse et al., "The Department of Homeland Security's Risk," 7, 16.

[33] Renn, "White Paper on Risk Governance: Towards an Integrative Framework," 63.

methodologies. This clearly illustrates the complexity of defining risk concepts and terms as they pertain to analysis, assessment, and management.

Haimes offers an illustration of how these three concepts — that of analysis, assessment and management — build on each other. Haimes claims that risk analysis is a prelude to assessment, and that the analyst must answer three questions: 1) What can go wrong? 2) What is the likelihood that it will go wrong? 3) What are the consequences if it does go wrong? The answers to these questions help to identify, quantify, and evaluate risk and the potential impact. Risk assessment, a prelude to risk management according to Haimes, builds on the analysis by seeking answers to a second set of questions: 1) What can be done and what options are available? 2) What is the trade-off in terms of cost, benefit, and risk? 3) What will the impact of the current decision be on future options? [34, 35]

The Government Accountability Office (GAO) has defined risk assessment as the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. According to the GAO, risk assessment is a coalescence of threat, vulnerability, and consequence. A risk assessment may include scenarios in which two or more threats interact to create a greater or lesser effect. A risk assessment provides the basis for the rank ordering of risks, and for establishing priorities for countermeasures.[36] Viewing both Haimes and the GAO's definitions, it seems that risk analysis is the building block and prelude to the overall risk assessment. Whether the analysis is done qualitatively or quantitatively, the end result supports the risk assessment.

According to DHS, in the absence of pure tactical intelligence, the assessment of risk benefits from a rich and voluminous set of data, which can be mined for patterns of historical behavior, and can translate into the projection of likely threat scenarios

[34]. Paczkowski, *Risk Management*, 15.

[35] Yacov Y. Haimes, "Roadmap for Modeling Risks of Terrorism to the Homeland," 35-41.

[36] Government Accountability Office, *Risk Management – Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure* (Washington, DC: Government Accountability Office, December 2005), 111.

involving categories of assets and/or geographic areas.[37] For the purpose of this paper, and taking into account Haimes, GAO and DHS concepts of analysis and assessment, a risk analysis was conducted for the passenger rail transportation system in New York and New Jersey. A scenario was drawn from the analysis, with the intention of using the scenario to evaluate the utility of the risk management/governance framework as a decision-making support structure.

B. RISK MANAGEMENT AND THE DECISION-MAKING PROCESS

1. Introduction

Recent legislation, national strategies, and public statements of government officials all call for the use of risk management as the cornerstone of the nation's effort to protect its critical infrastructure, and to inform decision making in homeland security.[38] Even in the most recent release of the National Strategy for Homeland Security, there is a clear emphasis on applying a comprehensive approach to risk management.[39] This approach requires that we understand how to effectively manage risk and to identify the elements of risk management that will assist with decision-making process. Each of the risk management frameworks analyzed for this study outline a method that engages the decision-making process, and enables the decision maker to make well-informed choices relative to risk.

2. The "Wickedness" of Decision Making in the Homeland Security Environment

Risk is clearly a factor that must be taken into account when making homeland security decisions, but it is only one of several factors that must be considered. In

[37] Masse et al., "The Department of Homeland Security's Risk," 16.

[38] Edward J. Jopek and Kerry L. Thomas, *Security Risk Management: Implementing a National Framework for Success in the Post 9/11 World.* Appeared in a Monograph from the George Mason University School of Law's entitled, "Critical Infrastructure Protection: Elements of Risk" (December 2007), 1.

[39] George W. Bush, *National Strategy for Homeland Security*, Washington, DC: The White House, October 2007, 1.

Lieutenant Colonel Dennis T. Gyllemsporre's article, "Decision Navigation: Coping with 21st-Century Challenges in Tactical Decision Making," he refers to John Von Neumann's classic analytical decision-making process as a starting point for decision-making theory. According to Von Neumann, the decision maker ideally behaves in a strictly rational way to achieve the best results. This method has five steps:

1. Identify the problem.
2. Generate alternative solutions.
3. Evaluate and choose between alternatives.
4. Implement the chosen solution.
5. Maintain the solution by monitoring, reviewing, and appraising the situation.

Gyllemsporre believes the model is robust, especially if feedback loops are added to support connectivity between each of the steps. However, the model also assumes the decision maker possesses perfect knowledge, perfect rationality, all of the information required to make decisions, and the ability to make those decisions without using any human values, prejudices, or emotions.[40]

Ross illustrates the homeland security decision-making environment by blending the factors of complexity and a high degree of uncertainty that are endemic to homeland security with the idea of "wicked problems."[41] The person who coined the term "wicked problem" was Horst Rittel. As Rittel defined it, wicked problems are distinguished by the following characteristics:[42]

- You do not understand the problem until you have developed a solution.
- Wicked problems have "no-stopping" rule.
- Solutions to wicked problems are not right or wrong.
- Every wicked problem is essentially unique and novel.
- Every solution to a wicked problem is essentially unique and novel.
- Every solution to a wicked problem is a "one-shot operation."

[40] Lieutenant Colonel Dennis T. Gyllensporre, "Decision Navigation: Coping with 21st-Century Challenges in Tactical Decision Making," *Military Review* (September/October 2003), 26.

[41] Robert Ross, *Risk and Decision-Making in Homeland Security*, 11.

[42] Jeff Conklin, "Wicked Problems and Social Complexity" (2006), 7, http://cognexus.org/wpf/wickedproblems.pdf [Accessed February 27, 2008].

- Wicked problems have no given alternative solutions.
- Every wicked problem can be a symptom of another problem.
- Any solution to a wicked problem will generate more problems.

According to Jeff Conklin, the author of, “*Wicked Problems and Social Complexity,*” there may be no solutions to wicked problems, or there may be a set of potential solutions that are devised, and another set of solutions that are never even considered.[43] He further asserts that it takes creativity to devise potential solutions, and that it is a matter of judgment to determine which solutions are valid, and should be pursued and implemented.[44] Conklin’s belief in the utility of creativity when devising potential solutions, and using sound judgment to determine validity is essentially at the core of homeland security decision making. It also supports the authors of the 9/11 Commission Report, who pointed to a lack of imagination as being one of the primary failures of pre-9/11 homeland security.[45]

Conklin also believes that decision makers must have a sense of what contributes to the “wickedness” of a problem. The following are examples of wicked problems and how they could be applied to passenger rail transportation:

- Screen every passenger or conduct random screening?
- Screen every passenger and cause extensive delays in commuter operations?
- Identifying a threat when there is a great deal of intelligence, but nothing specific.
- Identifying a threat when there is no credible intelligence targeting passenger rail.
- Identifying the appropriate response when there is tactical intelligence of a threat targeting passenger rail, and that intelligence is specific to cell operations?

[43] Masse et al., “The Department of Homeland Security’s Risk,” 4.

[44] Conklin, “Wicked Problems and Social Complexity,” 8.

[45] 9/11 Commission Report: *Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton & Co., 2004), 339.

Ross developed a model illustrating the difficulty of decision making in homeland security. Figure 2: Homeland Security Decision-Making Environment, blends the complexity and uncertainty of risk with the idea of wicked problems and social complexity.[46] His intention is to illustrate why the political aspects of homeland security problems can be so difficult to master.[47, 48]

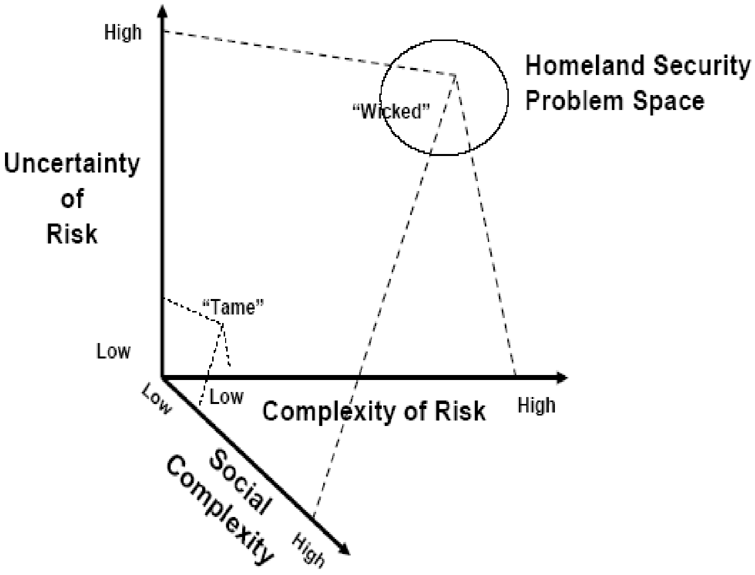


Figure 2. Homeland Security Decision-Making Environment[49]

[46] Robert Ross, *Risk and Decision-Making in Homeland Security,*12.

[47]Ibid., 11.

[48] The lower portion of the model offered by Ross, identifies Social Complexity as being very high when engaged with a wicked problem. This is based on theory regarding "wicked problems" offered by Horst Rittel and Melvin Webber. Rittel and Webber believe that, as distinguished from problems in the natural sciences, which are definable and separable and may have solutions that are findable, the problems of governmental planning – and especially those of social or policy planning – are ill defined; and they rely upon elusive political judgment for resolution. Social problems are never solved. At best they are only re-solved – over and over again.

[49] Robert Ross, "Risk and Decision Making in Homeland Security," 13.

3. Analytical and Intuitive Decision Making in the Homeland Security Environment

Modern approaches to the study of decision making have shifted focus and adopted a more integrated approach. This is illustrated in the Military Decision-Making Process (MDMP), which recognizes two methodologies that drive the decision-making process: Analytical Decision Making and Intuitive Decision Making.[50] According to the U.S. Army's Field Manual (FM 5-0), analytical decision making approaches a problem systematically. Leaders analyze a problem, generate several possible solutions, analyze and compare the solutions to a set of criteria, and then select the best solution. This approach is methodical and works well in complex or unfamiliar situations because it allows the breakdown of tasks into recognizable elements. It ensures that the commander and staff consider, analyze, and evaluate all relevant factors. It is an appropriate method to use when there is time to analyze all facets of the problem and its solution. Because it does take time, it may not be the appropriate method to use when circumstances require immediate decisions.[51]

The second methodology discussed in the FM 5-0 is Intuitive Decision making, which it describes as the act of reaching a conclusion by using pattern recognition that is grounded in knowledge, judgment, experience, education, intelligence, boldness, perception, and character. It is faster than analytic decision making because decisions are based on an assessment of the situation, rather than a comparison of multiple courses of action. It is used when time is short or when the speed of decision is important. It relies on the experienced leader's ability to recognize the key elements and implications of a particular problem or situation, reject the impractical, and select an adequate (rather than the optimal) course of action. Intuitive decision making significantly speeds up the decision-making process. It does not, however, work well when a situation includes

[50] The MDMP was chosen for this research due to the similar decision making processes that are evident within the homeland security environment. That being strategic, operational, tactical, analytical, and intuitive decision making. Each one of these decision making processes is reflective within the MDMP, and are applied during the risk management framework analysis.

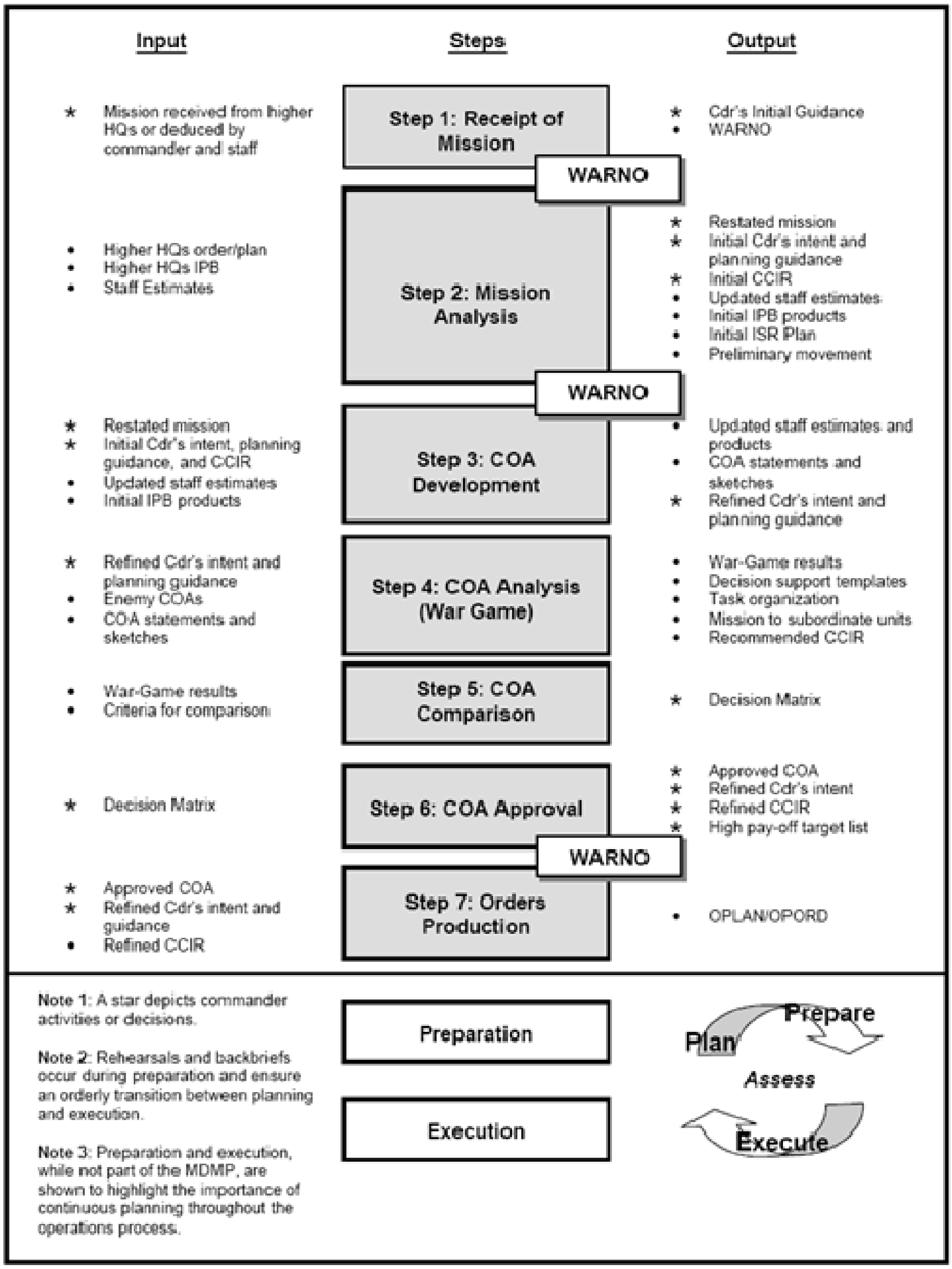
[51] U.S. Department of the Army, "Army Planning and Orders Production," 1-21.

inexperienced leaders, complex or unfamiliar situations, or competing courses of action. Additionally, substituting assessment for detailed analysis means that some implications may be overlooked. Commanders use intuitive decision making when time is short and the problems are straightforward. It is usually appropriate during execution.[52]

The MDMP model illustrated in Figure 3 represents the steps to achieving optimal decision making. However, according to Karol G. Ross et al., little guidance exists on how to abbreviate the process.[53]

[52] U.S. Department of the Army, "Army Planning and Orders Production," 1-21.

[53] Karol G. Ross et al., "The Recognition-Primed Decision Model," *Military Review* (July/August 2004), Military Module, 6.



Input	Steps	Output
★ Mission received from higher HQs or deduced by commander and staff	Step 1: Receipt of Mission	★ Cdr's Initial Guidance • WARNO
	WARNO	
• Higher HQs order/plan • Higher HQs IPB • Staff Estimates	Step 2: Mission Analysis	★ Restated mission ★ Initial Cdr's intent and planning guidance ★ Initial CCIR • Updated staff estimates • Initial IPB products • Initial ISR Plan • Preliminary movement
	WARNO	
★ Restated mission ★ Initial Cdr"s intent, planning guidance, and CCIR • Updated staff estimates • Initial IPB products	Step 3: COA Development	• Updated staff estimates and products • COA statements and sketches ★ Refined Cdr's intent and planning guidance
★ Refined Cdr's intent and planning guidance • Enemy COAs • COA statements and sketches	Step 4: COA Analysis (War Game)	• War-Game results • Decision support templates • Task organization • Mission to subordinate units • Recommended CCIR
• War-Game results • Criteria for comparison	Step 5: COA Comparison	★ Decision Matrix
★ Decision Matrix	Step 6: COA Approval	★ Approved COA ★ Refined Cdr's intent ★ Refined CCIR ★ High pay-off target list
	WARNO	
★ Approved COA ★ Refined Cdr's intent and guidance • Refined CCIR	Step 7: Orders Production	• OPLAN/OPORD

Note 1: A star depicts commander activities or decisions.

Note 2: Rehearsals and backbriefs occur during preparation and ensure an orderly transition between planning and execution.

Note 3: Preparation and execution, while not part of the MDMP, are shown to highlight the importance of continuous planning throughout the operations process.

Figure 3. MDMP Decision Making Model[54]

[54] U.S. Department of the Army, "Army Planning and Orders Production," 21.

Gary Klein, the author of *Sources of Power: How People Make Decisions,* has conducted research for military organizations for more than two decades, focusing on how individuals and organizations make decisions. According to Klein, intuitive decision making uses experience to recognize the patterns in a given situation.[55] The leader can quickly develop a course of action by employing mental war-gaming and pattern recognition learned through training, education and experience. The decision maker typically searches for the first course of action that will work in a given situation. It is experience and intuition that enable the leader to predict how a solution will work.[56] Klein refers to this process as the Recognition Primed Decision (RPD) Model. Figure 4 illustrates Klein's concept.

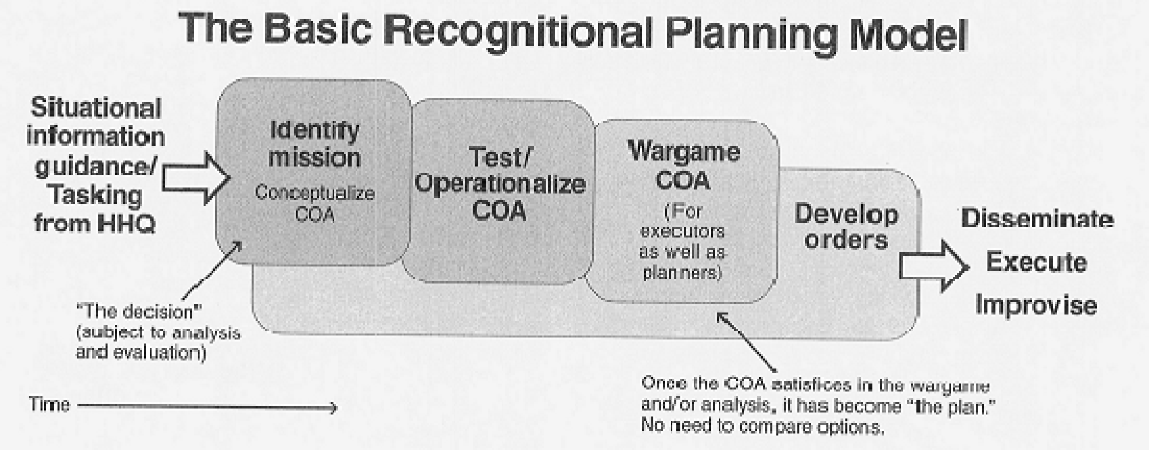

The Basic Recognitional Planning Model
Situational information guidance/ Tasking from HHQ
Identify mission
Conceptualize COA
Test/ Operationalize COA
Wargame COA
(For executors as well as planners)
Develop orders
Disseminate
Execute
Improvise
"The decision" (subject to analysis and evaluation)
Time
Once the COA satisfices in the wargame and/or analysis, it has become "the plan." No need to compare options.

Figure 4. Basic Recognition Planning Model[57]

[55] Gary Klein, *Sources of Power: How People Make Decisions,* Cambridge, Massachusetts: MIT Press, 1998, 24.

[56] David A. Bushey and Michael J. Forsyth, "The Recognition-Primed Decision Model: An Alternative to the MDMP for GWOT," *FA Journal* (January/February 2006), Military Module, 11.

[57] Karol G. Ross et al., "The Recognition-Primed Decision Model," *Military Review* (July/August 2004), Military Module, 7.

How can the analytical and intuitive principles of the MDMP model, integrated with the further in-depth, intuitive principles of the RPD model, assist with the decision-making process in an environment that is rife with wicked problems? Also, how do strategic, operational, and tactical levels of decision making figure into the environment of homeland security?

Strategic Decision Making: Strategic Decision Making requires that goals and objectives be developed for a strategic course of action. From a short-term perspective, strategic-level decisions rely on operational input, and provide the context for tactical operations. This level of strategic decision making is reflective during conflict or a progressing event. From a homeland security perspective that is focused on long-term strategies, these decisions are made with relatively low frequency since they tend to drive overarching capability creation. An example of creating an overarching capability would be to regulate and/or mandate private sector actions, such as requiring chemical facilities to increase security as a condition of remaining in business. Another example of strategic decision making comes from DHS, with its long-term funding commitments to specific geographic regions, as is the case with the Urban Area Security Initiatives (UASI).

Operational Decision Making: Operational Decision Making supports the strategic decision maker by implementing courses of action that support long-term strategic goals and objectives. The operational decision maker is required to ensure that operations can be carried out within existing capabilities. Operational and tactical-level decision making complement each other by linking operational plans to the deployment of resources that support strategic goals. An example would be an agency that has intelligence, gained through credible sources, that there is an immediate threat targeting the passenger rail transit system of New York and New Jersey. At the operational decision-making level, this would necessitate taking immediate preventive and protective measures at various transit nodes. The operational decision maker carries out these measures by identifying assets and technical entities, at the tactical level, that can assist in identifying the threat before it penetrates the passenger rail transit system.

Tactical Decision Making: Tactical Decision Making involves the employment of units, assets, and entities that can support the operational requirements of the mission.

In the example provided above, once the decision has been made to mobilize assets and technical entities, it is the tactical decision maker who initiates the action and the execution. This may require random bag searches conducted by law enforcement officers, and explosive detection K9s at every transportation node. The tactical decision maker carries out this deployment process, and maintains communication with operational decision makers.

The MDMP and RPD models contain principles that can assist with strategic, operational, and tactical level decision making. The MDMP model assists the military field commander who is faced with strategic decisions which will drive operations and deploy the appropriate tactical elements. The analytical components of the MDMP model are a methodical process that serves well in complex and unfamiliar situations. These elements - complexity and unfamiliarity - are reflective of wicked problems. The MDMP's analytical approach also serves well when time is available to analyze all aspects of a problem and its solution. It is particularly applicable in the intelligence community, where time is often available to cycle data through the intelligence analysis process. In the event that actionable intelligence emerges, the analytical approach allows the decision maker to thoroughly evaluate the situation before considering a course of action (see Figures 5).[58]

[58] Figure 5 is meant to illustrate the complexity in homeland security as it relates to intelligence driven decision making. Figure 5A is meant to provide a snapshot of the agencies who makeup the intelligence community. Figure 5B represents sources in which intelligence and data is collected from (acronyms are spelled out in list of acronyms and abbreviations). Figure 5C offers an intelligence process that is currently utilized by the New Jersey State Police.

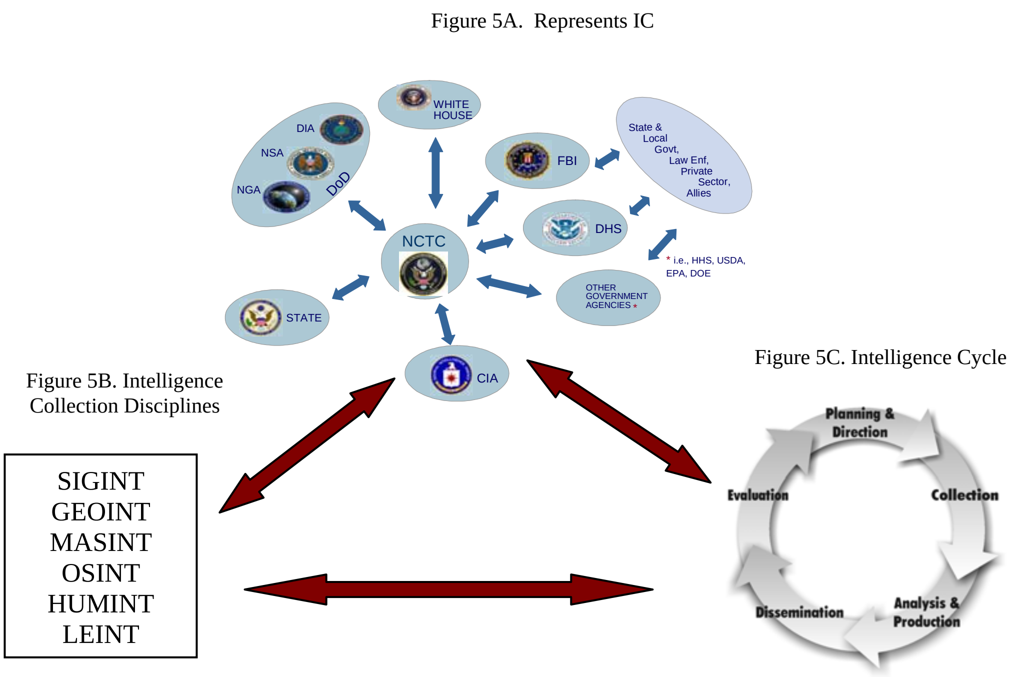


Figure 5A. Represents IC

Figure 5B. Intelligence Collection Disciplines

Figure 5C. Intelligence Cycle

Figure 5. IC Wicked Problem

The RPD model is based on intuition. Klein refers to intuition as depending on the use of experience to recognize key patterns that indicate the dynamics of a situation.[59] Recognizing key patterns through experience, and making decisions based on them certainly pertains to operational and tactical decision making. In the current domain of homeland security, however, the reliance is on national priorities, national frameworks, and scenario models that are intended to make up for a lack of experience, and are generally designed to assist with strategic level decision making. This is at the fault of no one. Homeland security is a fairly new concept. It is driven by many factors that create a great deal of flexibility in the decision-making process. The intuition can be gained through understanding the motives, intent, and capabilities of terrorists. Klein asserts that

[59] Gary Klein, *Sources of Power*," 31.

examining a situation can create an awareness of typical ways of responding.[60] Decision makers are also educated through exercises that allow for decisive and reactionary decision making.

Referring back to the example of wicked problems associated with the intelligence community, as illustrated in Figure 5, the intuitive approach of an FBI agent represents the agent’s experience with a particular (HUMINT) source that led to the identification of individuals developing peroxide-based explosives. The reliability of the source, coupled with the agent’s experience, can engage the intuitive process.

The principles of analytical and intuitive decision making can influence the response to an identified risk. Traditionally, there are four ways to respond: avoid it, mitigate it, transfer it, or accept it.[61] For example, a vessel destined for a U.S. port may contain biological contaminants. Does the decision maker avoid the risk by not accepting the vessel into a U.S. port, and transfer the risk by rerouting it to another destination? Does the decision maker accept the risk by allowing the vessel to dock in a U.S. port, and then attempt to identify the biological contaminants in order to identify its origin and developer? Analytical decision making will rely on the tactical intelligence provided to the decision maker, whereas the intuitive decision-making process is more reflective of how the decision maker executes the intercept of the vessel.

Each of the risk management frameworks are inclusive of strategic, operational, tactical, analytical, and intuitive decision making. Each share dependencies with one another. How the decision-making process is applied relies on the situation. If it requires strategic decision making, a more analytical approach may be more useful, whereas operational and tactical decision making require a blend of the two. In the next segment, we examine risk management and how it can improve capabilities in the homeland security environment.

[60] Gary Klein, *Sources of Power*,” 92.

[61] Robert Ross, “Risk and Decision Making in Homeland Security,” 3.

4. Risk Management and Capability Enhancement

According to Ross, risk management is a collective term for actions taken to either reduce the probability of an adverse event occurring, and/or to minimize the consequences. The steps included in risk management include identification of potential adverse events; assessment of the associated probability and consequences (i.e., risk); selection of appropriate risk-reducing actions; communicating the necessary risk information to those who need it; implementing risk mitigation actions; and monitoring the effectiveness of the actions taken.[62] Ross's definition captures the core elements of the risk management process that, for the most part, are components of the risk management frameworks used in this study.

David J. Kaufman, during a presentation at the Naval Postgraduate School, discussed how risk analysis and risk management accommodate one another: "Risk analysis is the process by which risks are identified and evaluated, whereas, risk management is the suite of actions taken to actually influence risk identified through the analytical process."[63] As Kaufman put it, risk is identified through analysis, which in turn drives the decision-making action in the risk management process. Identified risks can allow for effective decision making if the capabilities and resources are sufficient to drive the risk down. A national effort is underway to increase the U.S. capabilities via a strategy that places risk management at its core.

As states move forward with the development of State Preparedness Plans, they are using the guidance of the Target Capabilities List (TCL), which is intended to support the National Preparedness Goal (see Table 1: Target Capabilities List). The TCL provides a guide for development of a national network of capabilities that will be available when and where they are needed to prevent, protect against, respond to, and recover from major

[62] Robert Ross, "Combating Terrorism with Risk-Based Strategies," working paper for the Office of Comparative Studies Department of Homeland Security Science and Technology Directorate, 2007.

[63] David J. Kaufman, Presentation on "Planning for Homeland Security," Director for Preparedness Policy, Planning & Analysis, Department of Homeland Security, Naval Postgraduate School, Monterey, CA (October 10-11, 2007).

events.[64] In the category of "Common Capabilities" is "Risk Management," the foundation on which the "Mission Categories" of Prevention, Protection, Response, and Recovery, are built. The TCL also offers an outcome element that emphasizes the utility of risk management as a planning construct that supports effective prioritization and oversight of homeland security programs.[65]

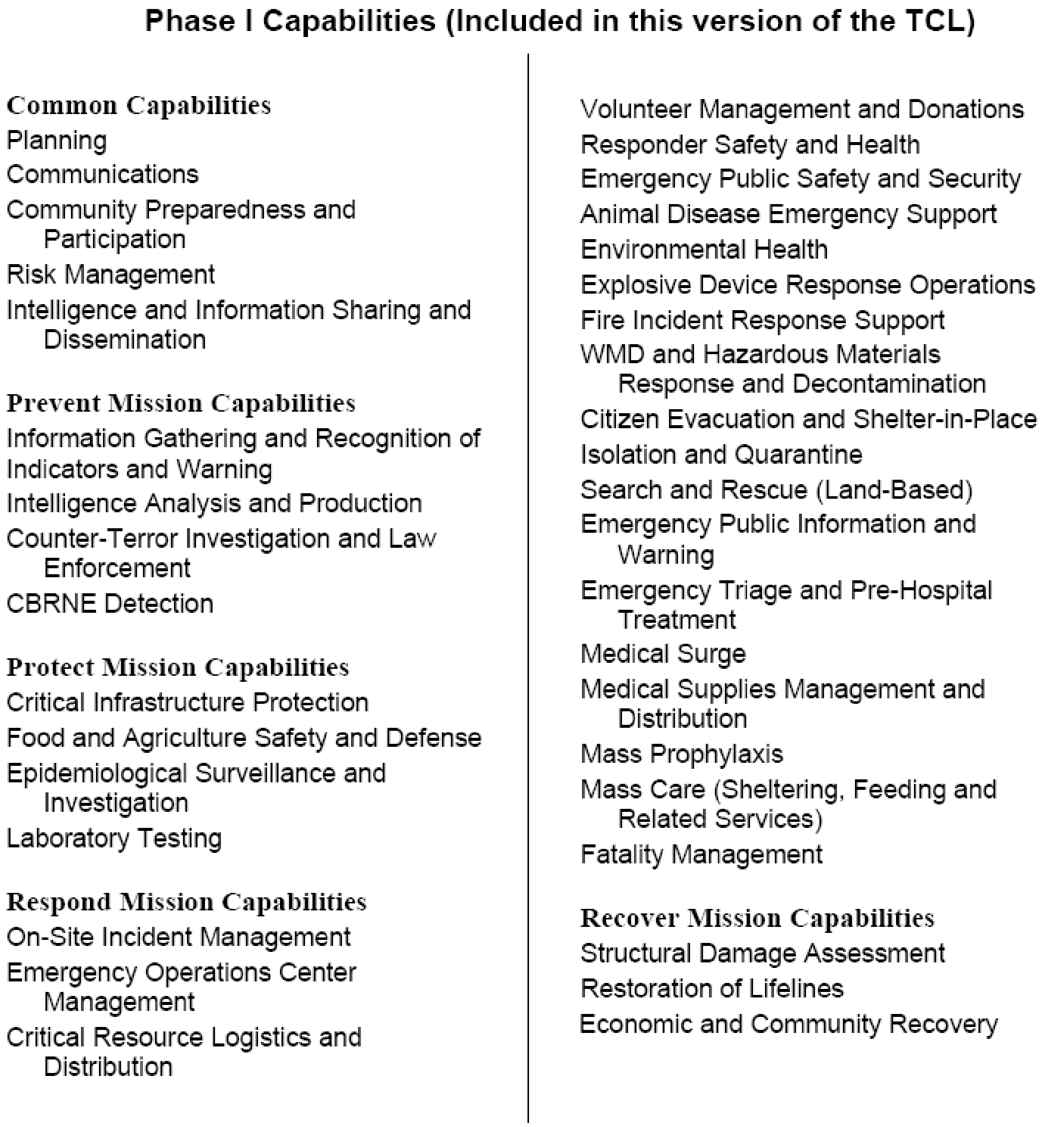
The TCL refers to the GAO for a common and usable definition of risk management: "A continuous process of managing—through a series of mitigating actions that permeate an entity's activities—the likelihood of an adverse event and its negative impact." Risk management is grounded in the capacity of all levels of government to identify and measure risk prior to an event, and, based on threats/hazards, vulnerabilities, and consequences, devise a plan that enables leadership to manage exposure to the threat by prioritizing and implementing risk-reduction strategies. The capability and actions required to perform risk management may vary between levels of government, but the foundation of risk management is constant.[66]

[64] Target Capabilities List: A companion to the National. http://www.emaponline.org/ [Accessed on February 20, 2008].

[65] Target Capabilities List: A companion to the National Preparedness Goal, 96.

[66] Ibid., 95.

Table 1. Target Capabilities List[67]



Phase I Capabilities (Included in this version of the TCL)

Common Capabilities
Planning
Communications
Community Preparedness and Participation
Risk Management
Intelligence and Information Sharing and Dissemination

Prevent Mission Capabilities
Information Gathering and Recognition of Indicators and Warning
Intelligence Analysis and Production
Counter-Terror Investigation and Law Enforcement
CBRNE Detection

Protect Mission Capabilities
Critical Infrastructure Protection
Food and Agriculture Safety and Defense
Epidemiological Surveillance and Investigation
Laboratory Testing

Respond Mission Capabilities
On-Site Incident Management
Emergency Operations Center Management
Critical Resource Logistics and Distribution
Volunteer Management and Donations
Responder Safety and Health
Emergency Public Safety and Security
Animal Disease Emergency Support
Environmental Health
Explosive Device Response Operations
Fire Incident Response Support
WMD and Hazardous Materials Response and Decontamination
Citizen Evacuation and Shelter-in-Place
Isolation and Quarantine
Search and Rescue (Land-Based)
Emergency Public Information and Warning
Emergency Triage and Pre-Hospital Treatment
Medical Surge
Medical Supplies Management and Distribution
Mass Prophylaxis
Mass Care (Sheltering, Feeding and Related Services)
Fatality Management

Recover Mission Capabilities
Structural Damage Assessment
Restoration of Lifelines
Economic and Community Recovery

Risk management and decision making are clearly at center stage when it comes to identifying risks, the capability requirements they generate, and the strategy for meeting those requirements. By enhancing capabilities through asset development, products, processes, and systems, it is possible to drive down risk for a given sector. An

[67] Target Capabilities List: A companion to the National Preparedness Goal, vii.

example would be improving U.S. protection and prevention capabilities through a robust information- and intelligence-sharing network. This network could be established through statewide fusion centers, or through an intelligence-based management system that allows law enforcement entities to share information. Developing an intelligence-sharing capability may help the decision maker throughout the risk management process, simply by knowing such a capability exists.

Figure 6, which is a variation of a graphic created by David Kaufman of DHS, illustrates the Likelihood of Event and Impact of Event with notional threats plotted in the upper right quadrant. The arrows represent the Mission Capabilities that, if in fact are enhanced, can drive the (IED Attack on Passenger Rail Train) down toward Residual Managed Risk. Thus, this improves our ability to manage risk and make better-informed decisions that can reduce the likelihood and impact of an event.

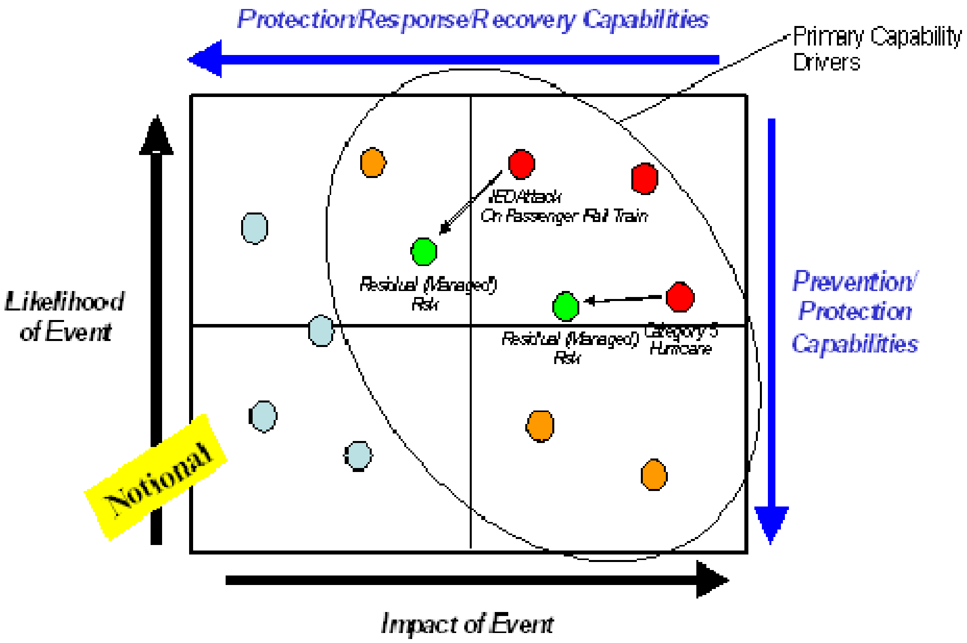

Protection/Response/Recovery Capabilities
Primary Capability Drivers
IED Attack On Passenger Rail Train
Residual (Managed) Risk
Residual (Managed) Risk
Category 5 Hurricane
Likelihood of Event
Prevention/ Protection Capabilities
Notional
Impact of Event

Figure 6. Driving Down Risk Through Capability Enhancement[68]

[68] Kaufman, Presentation on “Planning for Homeland Security.”

THIS PAGE INTENTIONALLY LEFT BLANK

III. RISK MANAGEMENT FRAMEWORK ANALYSIS

A. OVERVIEW OF THE RISK MANAGEMENT FRAMEWORKS AND THE DECISION-MAKING PROCESS

1. Introduction

This chapter introduces the risk management frameworks utilized for this study, and to take a closer look at the components that formulate each of the frameworks. The GAO, NIPP, and IRGC frameworks provide a model that illustrates the risk-management process. Within each of the frameworks are the core components that define the process. The methodology for this analysis is to provide an overview of each phase illustrated in the risk-management framework, and to ascertain how each component factors into the decision-making process. For each component, the decision-making processes discussed in Chapter II provide the construct for the analysis. This analysis is meant to be seen through the lens of a homeland security decision maker as it pertains to terrorism. From the position of the decision maker, the framework is notionally applied as a preparedness strategy, a pending event, or a progressing situation. The proposed methodology is not intended for a specific threat targeting an identified sector or region. The methodologies, however, are explored later in this paper and applied to a threat to the passenger rail transportation sector for NY/NJ. In addition, elements that support each component are linked to the various decision-making processes. Examples are provided to show the relevance for that particular process.

2. The Government Accountability Office (GAO) Risk Management Framework

While there is widespread support for using risk management in homeland security programs and decision making, doing so is a complex task that has few precedents and, until recently, little specific guidance. To provide a basis for examining efforts to carry out risk management, the GAO developed a framework based on best practices and other criteria. The framework is divided into five phases: (1) Setting strategic goals and objectives, and determining constraints; (2) Assessing the risks; (3) Evaluating the alternatives for addressing the risks; (4) Selecting appropriate alternatives; and (5) Implementing the alternatives and monitoring the progress made and the results achieved (see Figure 7).[69] The GAO has used this framework to examine many programs, such as air cargo security, general aviation security, and surface transportation security.

According to Ross, the GAO cycle (Figure 7) has several virtues. The first is its simplicity. By omitting many of the details provided in other examples, the GAO graphic provides the clearest and most easily understood cycle. Its biggest advantage is that it explicitly illustrates that the risk-management process really starts with strategic goals, objectives, and constraints established in law and administrative policies.[70] It is also necessary to note that the GAO framework is essentially a decision-making process. For example, a Six Step Ethical Decision Making process offered by the Ethics Resource Center lists the following steps:

- Step 1: Define the Problem
- Step 2: Identify Alternatives
- Step 3: Evaluate the Alternatives
- Step 4: Make the Decision
- Step 5: Implement the Decision
- Step 6: Evaluate the Decision[71]

Steps 3, 4, 5, and 6 can most certainly equate to the GAO components of Alternatives Evaluation, Management Selection, and Implementation and Monitoring. Therefore, it is necessary to dig a bit deeper into what types of decision-making processes occur at what phases, identify core elements for each component, and evaluate how it correlates with the homeland security risk problem space.

[69] Government Accountability Office, *Homeland Security – Applying Risk*, 8-9.

[70] Robert Ross, “Risk and Decision Making in Homeland Security,” Attachment B.

[71] Ethics Resource Center, Plus: The Decision Making Process, www.ethics.org/resources/decision-making-process [Accessed on March 3, 2008].

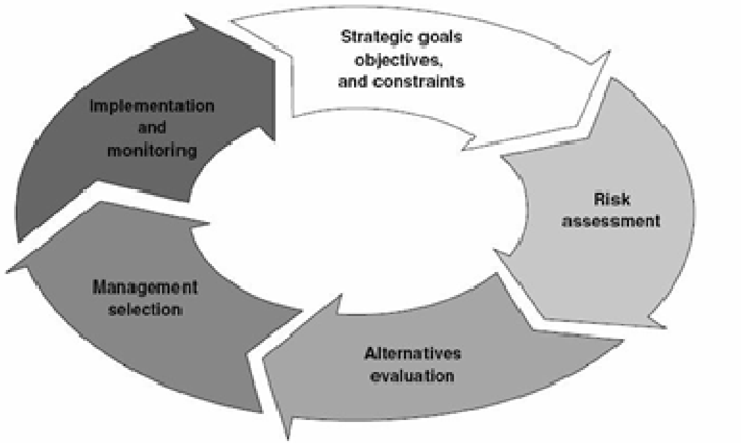

Strategic goals objectives, and constraints
Risk assessment
Alternatives evaluation
Management selection
Implementation and monitoring

Figure 7. GAO Risk Management Framework[72]

Strategic Goals, Objectives & Constraints

Strategic goals and objectives stimulate strategic decision making, and establish the foundation for the GAO risk management process. According to Henry Mintzberg, strategic decisions are those that determine the overall direction of an enterprise and its ultimate viability in light of the predictable, the unpredictable, and the unknowable changes that may occur in its most important surrounding environment.[73] The unpredictable and unknowable identified by Mintzberg is reflective of the problem space associated with homeland security due to uncertainty and complexity. However, direction that is reflective of the goals and objectives is still required from decision makers. Mintzberg adds that the goals and objectives state what is to be achieved and when results are to be accomplished, but they do not state how the results are to be achieved. The programs implemented to support the goals and objectives specify the step-by-step sequence of the actions that are necessary to achieve major objectives. They express how objectives will be achieved within the limits set by policy.[74] This component of the GAO framework is the foundation and support for the remaining components of the cycle.

[72] Government Accountability Office, *Homeland Security – Applying Risk*, 9.

[73] Henry Mintzberg and James B. Quinn, *The Strategy Process: Concepts and Contexts* (Englewood Cliffs, New Jersey: Prentice Hall, 1992), 5.

[74] Mintzberg and Quinn, *The Strategy Process*, 5.

(GAO) Strategic Goals Objectives and Constraints	
Strategic DM	This component is reflective of Strategic DM at its core, and can be applied to multiple homeland security issues and concerns that may cut across many sectors. Decision makers can benefit from identifying the strategic goals, objectives and constraints that would provide the most effective course of action and positive outcomes. It also provides a starting point in the framework that can identify assets, systems, networks, processes, and capabilities to support the goals and objectives.[75]
Operational DM	Premature in the process for Operational DM to be effective unless threat is imminent.
Tactical DM	Premature in the process for Tactical DM to be effective unless threat is imminent.
Analytical DM	Identify the analytical tools, processes, networks, and systems that can support the next component of the GAO framework, which is Risk Assessment. For example, intelligence and information sharing and dissemination through the utilization of a statewide fusion center would represent analytical tools, processes, networks, and systems.
Intuitive DM	Premature in the process for Intuitive DM to be effective.
Capability Based DM	The decision maker will rely a great deal on those capabilities that will support the strategic goals and objectives. If capabilities do not exist that can support the overall strategic goal, the decision maker may realize the constraints and redirect the strategy. For example, a threat targeting malls statewide with an Improvised Explosive Device (IED). The strategic goals and objectives must reflect whether the capability exists to detect and defend against such attacks.

Risk Assessment

- **Threats**
- **Vulnerabilities**
- **Criticality**

The GAO believes that the assessment of risk is a critical component of the risk management approach. In many GAO documents and testimonies related to homeland security risk and decision making, it is suggested that there are key elements fused to this component. The GAO identifies three key elements — threats, vulnerabilities, and criticality — that inform the decision-making process. According to the GAO, threat assessment identifies and evaluates potential threats on the basis of such factors as capabilities, intentions, and past activities. A vulnerability assessment identifies weaknesses that may be exploited by identified threats, and suggests options to address those weaknesses. A criticality

[75] These terms are utilized to represent operational functions of assets, systems, networks, and processes. They are not intended to be definitive in terms of identifying critical infrastructure that is evident in the NIPP. Examples in this case would be, a Fusion Center representing an asset; an intelligence cycle representing a process and a system; and an intelligence/information dissemination function linking federal, state, and local agencies would represent a network.

assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as its importance to public safety and the economy, as a basis for identifying which structures or processes are more important to protect from attack. Information from these three assessments can lead to a risk characterization, such as high, medium, or low, and provide input to the task of prioritizing security initiatives.[76]

This component of the framework includes the risk analysis that provides the analytical tools to support the overall risk assessment (although it is not illustrated in the framework). The GAO identifies threat, vulnerability, and criticality as key elements. It defines risk assessment as being qualitative and/or quantitative to assist in determining the likelihood of an adverse event occurring, its severity and impact, and the consequences. It may include scenarios under which two or more risks interact, creating greater or lesser impacts, as well as the ranking of risk events.[77] Risk assessment is inclusive of each of the decision-making processes shown in the table below.

[76] U.S. Government Accountability Office, *Transportation Security – Systematic Planning Needed to Optimize Resources* (Washington, DC: Government Accountability Office, February 15, 2005), 4.

[77] U.S. Government Accountability Office, *Rail Security – Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain* (Washington, DC: Government Accountability Office, March 23, 2004), Appendix I.

(GAO) Risk Assessment	
Strategic DM	The Risk Assessment Component builds on the goals and objectives, and provides the decision maker with a better understanding of situational awareness, the identity of root causes, and the determinants for a course of action. Through the lens of the Strategic DM, resource allocation for developing threat analysis, vulnerability analysis, and criticality analysis, as well as pre-planning, will rely heavily on a thorough risk-assessment process.
Operational DM	The Operational DM may rely on the products generated by the Risk Assessment that are specific to threats, vulnerability, and criticality and that are the essential elements of the component. These include, for example, threats targeting a critical sector, such as dams. Intelligence analysis and production will support the Operational DM by identifying which dams are most critical, and which operational elements are needed to prevent an attack.
Tactical DM	The Tactical DM relies on the Risk Assessment Component to identify adversarial capabilities. To support the example provided above, the Tactical DM may need to know how dams may be attacked to determine if tactical intervention and execution is required.
Analytical DM	The Risk Assessment Component directly reflects the Analytical DM process. The Analytical DM factors in assets, systems, networks, processes, and capabilities that are significant to the core elements, i.e., threat, vulnerability, and criticality. Analytical DM feeds off the risk assessment to make the best informed decision.
Intuitive DM	The Intuitive DM may identify with an element of the Risk Assessment Component that may necessitate immediate action. This could also cause the decision maker to skip the Alternative Evaluation and Management Selection components and transition into the Implementation and Monitoring Component (see Figure 7).
Capability Based DM	The Risk Assessment Component will drive Capability Based DM. Threat, vulnerabilities, and criticality are all linked to the mission areas and target capabilities discussed in Chapter II. Capability Based DM will rely on the risk assessment for the mission areas and target capabilities that will have the greatest impact in driving down risk.

Alternatives Evaluation

The GAO, in many of its documents, does not define the Alternatives Evaluation component of the framework. However, Alternatives Evaluation is an element of the decision-making process. It relies on the validity of the Risk Assessment Component. Yet once again, due to the uncertainty and complexity of the homeland security problem space, the Alternatives Evaluation Component must be flexible enough in the event the Risk Assessment Component produces unreliable products. Alternatives Evaluation does, however, affect the various levels of the decision-making processes outlined below.

(GAO) Alternatives Evaluation	
Strategic DM	Alternatives Evaluation would support the Strategic DM during the Strategic Goals, Objectives and Constraints Component if the problem was identified. However, during risk assessment, a different set of problems can surface causing a redirection in strategy. The Alternatives Evaluation Component provides a mid-point for the Strategic DM to re-evaluate the course of action.
Operational DM	The Operational DM can look to the Alternatives Evaluation Component as an assessment stage prior to deployment. The Operational DM may opt to develop alternatives based on the risk assessment.
Tactical DM	The Tactical DM will rely on the Alternatives Evaluation Component as an assessment stage prior to execution, and will closely coordinate with the Operational DM in the event an alternative course of action has been determined.
Analytical DM	Alternatives Evaluation supports the Analytical DM by providing time to review the products generated by the Risk Assessment Component. The Analytical DM may identify deficiencies and gaps in the risk assessment, and re-assess a particular element.
Intuitive DM	The Alternatives Evaluation Component can assist the Intuitive DM if there is an alternative course of action that the decision maker has experienced in the past and that had a positive outcome.
Capability Based DM	The Alternatives Evaluation Component may lead to a redirection in strategy. Therefore, Capability Based DM may need to revaluate assets, systems, and networks in order to support a refocused strategy.

Management Selection

To this point in the process, the three components of (1) Strategic Goals, Objectives and Constraints, (2) Risk Assessment, and (3) Alternatives Evaluatio*n* have been mutually dependent, engaging the decision-making process at various levels. It is the Management Selection Component that enables the decision maker to move forward with a course of action. As illustrated in the table below, this is the staging phase prior to implementation.

(GAO) Management Selection	
Strategic DM	The Strategic DM ensures that Operational, Tactical, Analytical and Capability Based decision makers understand the course of action, which should be based on the work done in the previous phases.
Operational DM	The Operational DM ensures that the Management Selection Component is adequate to deliver a positive outcome and the resources to mobilizes assets and engages networks, systems, and processes that will support the Implementation and Monitoring Component.
Tactical DM	The Tactical DM coordinates with the Operational DM to ensure interoperability and verifies management selection objectives.
Analytical DM	The Analytical DM preps the systems, networks, and processes that will be relied upon during the implementation and monitoring phase. For example, situational awareness for the Operational DM may rely on intelligence and information dissemination from a state fusion center.
Intuitive DM	The Intuitive DM reflects on prior experience and knowledge, and determines how the internal understanding of the problem can be met with a positive outcome based on the Management Selection.
Capability Based DM	Capabilities have already been determined, and are waiting to be implemented.

Implementation and Monitoring

This is the last component of the GAO risk management framework. The Implementation and Monitoring Component is critical to how a problem can be mitigated. Once again, in dealing with the uncertainty and complexity of the homeland security risk problem space, implementation needs to be closely monitored due to the dynamics that can perplex the decision-making process. The cyclical process inherent in the GAO framework allows the decision maker to transition back to the Strategic Goals, Objectives and Constraints Component if the components of implementation and monitoring deviate away from the original course of action set forth by the goals and objectives. In addition, what is apparent is that components in this decision-making process are dependent on one another, which means the decision maker relies on the continuous elements of the risk assessment to support operations.

(GAO) Implementation and Monitoring	
Strategic DM	The Strategic DM is reliant on the monitoring component. This is based on the fact that if the implemented strategy fails, the Strategic DM can transition back into developing strategic goals and objectives and develop another course of action. Monitoring is an essential element of the Risk Assessment Component, which can be processed through the various systems, processes, and networks.
Operational DM	The Operational DM is directly engaged in the Implementation and Monitoring Component. Operational DM relies on a continual risk assessment to improve situational awareness. The Operational DM is a consumer of intelligence and information, which can be generated from analytical tools and produce products to support decision making.
Tactical DM	The Tactical DM is directly engaged in the Implementation and Monitoring Component due to execution and action. Tactical DM relies on a continual risk assessment of the immediate operating environment. The Tactical DM maintains communication with the Operational DM to ensure the course of action is consistent with the strategic goals, and objectives.
Analytical DM	The Analytical DM supports the Operational DM and Tactical DM by generating products through intelligence and information gathering processes and systems. Therefore, a continuous risk assessment focused on the recognition of indicators and warnings is paramount.
Intuitive DM	It is in this component of the framework that Intuitive DM can be adopted and acted upon. The Operational, Tactical, Analytical, and Capability Based decision makers are all engaged at the Implementation and Monitoring Component. The Intuitive DM emphasizes pattern recognition based on knowledge, judgment, experience, education, intelligence, boldness, perception, and character. The dynamics of an unfolding event may trigger pattern recognition and necessitate an immediate change in the course of action.
Capability Based DM	Capability Based DM is closely monitored by all those who are engaged in utilizing the assets, systems, and networks to support the course of action.

The GAO has suggested in many of its reports that by building a robust risk management framework, homeland security decision making can be improved dramatically. It further suggests that "risk management is the best approach to guide programs and responses to better prepare against terrorism and other threats."[78] The GAO framework is simplistic, and merely offers a starting point for the decision-making process. It reflects a cyclical decision-making process, with each component offering guidance to the decision maker.

Clearly reflective in the decision-making process tables was the inclusion and reliance on the Risk Assessment Component and its core elements of threat, vulnerability,

[78] U.S. Government Accountability Office, *Homeland Security – A Risk Management Approach can Guide Preparedness Efforts* (Washington, DC: Government Accountability Office, October 31, 2001), 11.

and criticality. The decision-making process was dependent on the Risk Assessment Component to guide decisions through the entire framework. The GAO has emphasized the importance of risk assessment as the centerpiece of its risk management process. GAO suggests that, after threat, vulnerability, and criticality assessments are completed and evaluated in a risk-based decision process, key actions can be taken to better prepare against potential attacks or events. The GAO also says that threat assessments alone are insufficient to support key decisions; leaders and managers can make better decisions if they use a risk management approach in conjunction with vulnerability and criticality assessments.[79]

Although the decision-making process tables are meant to reflect how decision making is executed using the components of the GAO framework — with the exception of the Risk Assessment Component — there has been little support by the GAO indicating how the other components of the risk management framework interact with the decision maker.

3. The National Infrastructure Protection Plan (NIPP) Risk Management Framework

The NIPP has been described as a base plan or national blueprint for how DHS, sector-specific agencies, and other relevant stakeholders should coordinate critical infrastructure and key resource-protection initiatives.[80] As has been previously stated, adoption of a risk-management framework is essential for DHS to assess risk, determine which elements should be addressed within available resources, and set homeland security priorities.[81] Central to the entire concept of the NIPP, and at the heart of sector planning and implementation efforts, is the NIPP's risk-management framework. That

[79] *Homeland Security – A Risk Management Approach can Guide Preparedness Efforts*, 12.

[80] John P. Paczkowski, "Risk Management as Strategic Change in National Homeland Security Policy," Naval Postgraduate School Thesis, September 2007, 50.

[81] Government Accountability Office, *Homeland Security – Applying Risk,* 3.

framework establishes basic principles and criteria for assessing the vulnerability of critical infrastructure and key resources, and formulating and managing the implementation of security strategies.[82]

The cornerstone of the NIPP is its risk management framework. NIPP defines risk as the combination of the frequency of occurrence, vulnerability, and the consequence of a specified hazardous event. In the context of the NIPP, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.[83] The NIPP risk-management framework establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific (meaning transportation, energy, water) risk that drives infrastructure protection activities. The framework applies to the general threat environment, as well as to specific threats or incidents. The NIPP risk management framework illustrated in Figure 8 includes the following activities: (1) Set security goals; (2) Identify assets, systems, networks, and functions; (3) Assess risk; (4) Prioritize; (5) Implement protective programs; and (6) Measure effectiveness.

The NIPP utilizes the risk management framework as part of the overall effort to ensure a steady state of protection within and across the critical infrastructure/key resource sectors. DHS, the various sector-specific agencies and their security partners share responsibility for implementation of the NIPP risk management framework. Sector-specific agencies are responsible for leading sector-specific risk management programs, and for ensuring that the tailored, sector-specific application of the risk management framework is addressed in their respective sector-specific plans.[84]

The NIPP offers a more detailed description of how the NIPP risk-management framework can assist with the decision-making process. While the GAO offered a broad,

[82] U.S. Department of Homeland Security, *National Infrastructure Protection Plan – Executive Summary* (Washington, DC: U.S. Department of Homeland Security, 2006), 1-5.

[83] Ibid., 29.

[84] Ibid., 30.

simplistic framework, the NIPP digs deeper into the core elements of each component to learn how they apply to the decision-making process.

The methodology for the analysis will remain the same. Each component is examined through the eyes of the homeland security decision maker. The component represents the phase or stage within the framework; the core elements represent the foundation upon which the component is built. The analysis will also identify commonalities and distinct differences between the NIPP and the GAO processes.

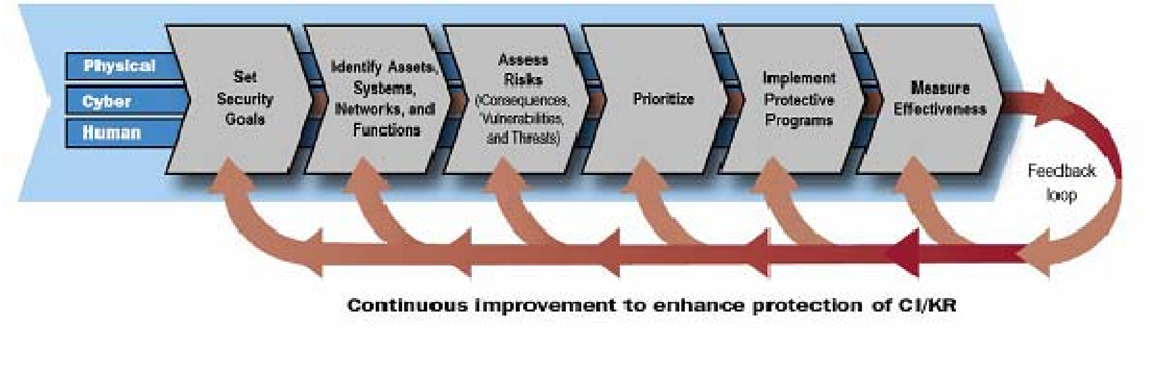

Physical
Cyber
Human
Set Security Goals
Identify Assets, Systems, Networks, and Functions
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Protective Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CI/KR

Figure 8. NIPP Risk Management Framework[85]

Set Security Goals

The NIPP describes this component as a way to define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture. This description is based on the achievement of a robust, protected, and resilient infrastructure requiring national and sector-specific homeland security goals that collectively represent the desired security posture.[86] The NIPP further outlines descriptive elements to support the Set Security Goals Component of the framework by narrowing the scope and focusing on security goals as they relate to sectors. The bullets below are viewed from a sector perspective representing security goals and their related supporting objectives:

[85] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2006, 29.

[86] Ibid., 31.

- Define the protective (and, if appropriate, the response or recovery) posture that security partners seek to attain;
- Express this posture in terms of objective metrics and the time required to attain it through specific supporting objectives;
- Consider distinct assets, systems, networks, operational processes, business environments, and risk management approaches;
- Vary according to the specific business characteristics and security landscape of the affected sector, jurisdiction or locality.

The NIPP refers to the above items from a collective standpoint, suggesting that these goals can guide all levels of government and the private sector in tailoring protective programs and activities to address CI/KR protection needs.[87] The NIPPs support for this component is clear in the elements provided above. The NIPP lays out a foundation in which this component can be reflective. The four elements described above enhance decision making, particularly for the Strategic DM. This was not the case in the GAO model, which left the decision maker to determine how goals and objectives were to be decided. There is also more description for the decision maker in setting security goals.

[87] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 29.

(NIPP) Set Security Goals	
Strategic DM	The Strategic DM can find utility in each element of the Set Security Goals Component for developing a COA. The elements build upon one another, and can benefit the Strategic DM for both long-term and short-term goals. As an example, the first element is to define the protective (and, if appropriate, the response or recovery) posture that security partners seek to attain. The Strategic DM can identify what levels of protection are needed to, for example, safeguard chemical plants. The Strategic DM develop supporting objectives, and then consider distinct assets, systems, and networks that represent the operational processes needed to support objectives, and to conduct security for chemical plants in given a jurisdiction or locality.
Operational DM	Premature in the process for Operational DM to be effective unless threat is imminent. The Operational DM may offer guidance to the Strategic DM for appropriate response- or recovery-related missions.
Tactical DM	Premature in the process for Tactical DM to be effective unless threat is imminent. The Tactical DM may offer guidance to the Operational DM based on execution strategies for a given environment. An example would be levels of personal protective equipment (PPE) for entities responding to a chemical facility containing chlorine.
Analytical DM	The Analytical DM will support the security goals by identifying distinct assets, systems, networks, operational processes, business environments, and risk management approaches to best support the SSP.
Intuitive DM	Premature in the process for Intuitive DM to be effective.
Capability Based DM	Capability Based DM can set security goals based on specific business characteristics and the security landscape of a given sector, jurisdiction or locality. The Capabilities can then be defined as through MAs and TCs.

Identify Assets, Systems, Networks, and Functions

To meet its responsibilities under the Homeland Security Act and HSPD-7, DHS maintains a comprehensive national inventory of the information needed to identify those assets, systems, networks, and functions that make up the nation's CI/KR. This information may be different for each sector because it is collected on an asset, system, network, or function basis, as determined by the fundamental characteristics of each sector.[88] DHS compiles the inventory in a manner that enables it to be quickly scanned, searched, and analyzed. This allows DHS to rapidly identify the assets, systems, networks, or functions that may be the subject of emergent terrorist statements or interest. DHS maintains the inventory in the National Asset Database (NADB) that is meant to be used as support to

[88] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 31.

domestic incident management by helping to inform decision making, establish strategies for response, and identify priorities for restoration, remediation, and reconstruction.

According to a Congressional Research Service Report, many critics of the NADB have assumed that it is (or should be) DHS’s list of the nation’s most critical assets. According to the report, critics are concerned that the database, in its current form, is being used inappropriately, as the basis upon which federal resources, including infrastructure protection grants, are allocated. DHS refutes these assumptions and characterizes the NADB not as a list of critical assets, but rather as a national inventory from which various lists of critical assets are produced. As such, DHS maintains that the database is just the first step in its risk-management process as outlined in the NIPP.[89]

The utility of the NADB can assist the decision maker. If the creators of the database intended to support incident management decision making, the NADB should be current, and populated in a manner suggested in the NIPP, i.e., by using a bottom-up and top-down approach. The bottom-up approach should include an aggregate assessment at the facility level with regard to both on-site and off-site consequences to the facility’s mission, as well as the surrounding population, that could result from natural disasters, accidents, or terrorist attacks. A top-down approach normally includes an assessment of key missions, and the identification of high-level processes, capabilities, and functions on which those missions depend.[90]

The Identify Assets, Systems, Networks, and Function Component (IASNF) was not a component of the GAO framework. From the contents of the NIPP, we are able to extract the elements that support this component of the NIPP framework. It is also important to note the context in which IASNF is utilized. Throughout this paper, assets, systems, networks, and functions are referred to as operational elements (see footnote 7). In this sense, they represent CI/KR. The elements below will assist with the analysis of the decision-making processes table.

[89] Congressional Research Service, *Critical Infrastructure: The National Asset Database* (Washington, DC: Congressional Research Service, September 14, 2006), Summary.

[90] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2006, 32.

- System components that are essential to the infrastructure mission and function;
- Dependencies and interdependencies (i.e., what an asset depends on in order to function, and which assets are reciprocally dependent upon it);
- Specific information on the asset, system, network or function needed to support consequence analysis;
- Assessment information that would enable DHS to conduct further comparative risk analysis in cooperation with SSAs, the private sector, other security partners, or subject matter experts.

(NIPP) Identify Assets, Systems, Networks, and Functions	
Strategic DM	The Strategic DM can use this component of the framework to further assist with developing goals, objectives, and setting a COA. Each element uniquely provides the Strategic DM with evidence of how to protect a particular category of critical infrastructure. The NADB would be an optimal starting point for the Strategic DM to outline the system components that are essential to the infrastructure mission and function. The Strategic DM can develop a COA based on this information and protect the most vital components of that particular infrastructure.
Operational DM	The Operational DM can review the assets, systems, networks, and functions for a particular set of critical infrastructure, and evaluate methods for deterring penetration and the detection of terrorist activity.
Tactical DM	The Tactical DM can also review the assets, systems, networks, and functions for a particular set of critical infrastructure, and to evaluate protective measures and response operations from a tactical perspective.
Analytical DM	The Analytical DM looks to the assets, systems, networks, and functions component to begin developing risk assessment strategies specific to critical infrastructure. The Analytical DM can extract pertinent information relative to system components essential for function, dependencies and interdependencies of an asset, and generate risk analysis products for the Assessment of Risk Component.
Intuitive DM	Premature in the process for Intuitive DM to be effective.
Capability Based DM	By identifying assets, systems, networks, and functions, the Capability Based DM can identify what TCs are essential for the prevention, protection, response, and recovery for a particular sector.

Assess Risks

- **Consequences**
- **Vulnerabilities**
- **Threats**

Various methodologies are available to facilitate risk assessment. Many owners and operators use risk assessment methodology as a component of their business continuity and disaster mitigation planning. A common approach based on a robust understanding of existing methodologies is needed to enable the setting of protection priorities across sectors.[91] The NIPP acknowledges that the first element of this approach is to establish a common definition and process for analysis of the basic factors of risk for CI/KR protection. In Chapter II, we recognized the relevance of these elements by identifying them in government documents, publications, and testimony from DHS Secretary Michael Chertoff. From this, we concluded that these core elements helped to establish a broader understanding of terrorism risk (see Figure 1). The NIPP identifies these elements within the Assess Risk Component as a function of consequence, vulnerability, and threat. Within each element exists baseline criteria that can assist the decision maker by way of assessment and analysis. For each of the elements, we will look at some of the suggested steps and tools offered by the NIPP that can assist the decision maker.

Consequence: This constitutes the negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged or disrupted by a terrorist attack, natural disaster, or other incident.[92]

In the NIPP framework, consequence is measured as the range of loss or damage that can be expected. Consequences that are considered at the national level are divided into four main categories:

- Human impact: Effect on human life and physical well-being (e.g., fatalities, injuries);
- Economic impact: Direct and indirect effects on the economy (e.g., cost to rebuild the asset, cost to respond to and recover from attack, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage);
- Impact on public confidence: Effect on public morale and confidence in national economic and political institutions;
- Impact on government capability: Effect on the government’s ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.[93]

[91] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 35.

[92] Ibid.

[93] Ibid.

These criteria provide the decision maker only with what is relative to consequences. A consequence assessment tool would certainly enhance the decision maker's ability to make better-informed decisions if the tool examined the inherent characteristics of assets, systems, or networks to identify worst-case consequences that are likely to result if the CI/KR in question is destroyed, incapacitated, or exploited. DHS is sponsoring the development of a suite of tools based on the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework that satisfies the baseline criteria for risk assessment, and can be used for national cross-sector risk assessment. This tool set enables owners and operators to calculate potential consequences and vulnerability to an attack using a consistent system of measurements. It also provides the means to convert and compare the results obtained from assessments performed with other suitable methodologies that are consistent with the NIPP baseline criteria.[94]

Vulnerability: This is the likelihood that a characteristic of, or a flaw in, an asset or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards.[95]

- Determining an appropriate vulnerability assessment strategy (e.g., self-assessment, state or federally led assessment, expert reviews, or independent third-party assessment);
- Identifying a methodology/tool appropriate for the particular type of asset, system, or network under consideration;
- Identifying and grouping vulnerabilities using common threat scenarios;
- Identifying dependencies and interdependencies with other assets and sectors;
- Considering vulnerabilities associated with physical, cyber, and human elements;
- Analyzing benefits of existing protective programs;
- Assessing residual gaps to determine unresolved vulnerabilities.

[94] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 37.

[95] Ibid.

An assortment of vulnerability-assessment approaches are used by the different CI/KR sectors. The primary vulnerability-assessment methodologies used in each sector are described in the respective SSPs. The SSPs also provide specific detail regarding how the assessments can be carried out (e.g., by whom, how often).[96] The vulnerability assessment can fulfill the many unanswered gaps that a decision maker may need to call upon prior to developing a preparedness strategy or COA. But, as stated in the consequence assessment, the tools that deliver the metrics and analysis provide support for the decision maker.

Threat: It is the likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk from a terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary. In the context of natural disaster or accident, the likelihood is based on the probability of occurrence.[97]

The remaining factor to be considered in the NIPP risk-assessment process is the analysis of threat. In the context of terrorist risk assessment, the threat component of the analysis is calculated based on the likelihood of a terrorist attack method on a particular asset, system, or network. The estimate of this likelihood is based on an analysis of intent and capability of a defined adversary. The incident management, disaster response, public safety, and other communities have developed and use various tools to estimate the threat of natural disasters and accidents. These tools include such analytical aids as the models used by the National Hurricane Center (NHC) to forecast hurricane landfall and the fault tree models used by the National Regulatory Commission (NRC) in nuclear power plant engineering analysis. Because similar models are not yet in broad use for terrorist threats, the NIPP provides an augmented framework for the terrorist aspects of threat analysis.[98]

To assist the decision maker, the NIPP identifies a tool and function that will funnel threat information and intelligence to homeland security leaders. The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated

[96] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2006, 38.

[97] Ibid., 35.

[98] Ibid., 38.

threat analysis for all CI/KR sectors.[99] HITRAC develops analytical products by combining intelligence expertise based on all-source information, threat assessment, and trend analysis, with practical business and CI/KR operational expertise informed by current infrastructure status and operations information. Tools such as HITRAC are being developed on a smaller scale at statewide fusion centers with the full intention of sharing critical threat analysis with infrastructure stakeholders.

The NIPP suggests that risk assessments for CI/KR protection consider all three components of risk, and are conducted on an asset, system, network or function basis, depending on the fundamental characteristics of the infrastructure being examined. The NIPP establishes baseline criteria for risk assessment methodologies that can provide a guide for improving the decision-making process. This component of the NIPP framework digs a lot deeper into the intricacies of each element, and even identifies tools and functions that can assist with the decision-making process.

Both the GAO and NIPP recognize the essential elements of risk assessment and place both of these components at the center of the risk management framework process. The context in which the elements are described in the NIPP make it easier for the decision maker to understand how risk assessment methodologies can be of assistance. The table below is meant to extract the core elements from the Assess Risk Component, and further enhance each of the decision-making processes.

[99] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2006, 40.

(NIPP) Assess Risks	
Strategic DM	The Assess Risk Component outlines the criteria from which the Strategic DM can draw. The elements of consequence, vulnerability, and threat, coupled with the suggested baseline criteria and tool enhancements, offer the Strategic DM a larger pool of relative risk assessment principles. A robust framework of risk assessment methodologies integrated with the appropriate tools for SSAs can assist with strategic decisions that are oriented toward preparedness strategies, resource allocations, and situational courses of action.
Operational DM	The Operational DM can make better informed decisions based on baseline criteria and tool enhancements. By understanding the elements of consequence, vulnerability, and threat through the principles of assessment and analysis suggested by the NIPP, the Operational DM can support a COA that may require a robust detection and deterrence mission by identifying and grouping vulnerabilities using common threat scenarios.
Tactical DM	The Tactical DM relies on assessing risks for identifying adversarial capabilities. As suggested through by the NIPP, tools such as HITRAC can assist the Tactical DM by identifying the most frequently used methods of attack by terrorists for a given sector.
Analytical DM	The Analytical DM process would rely on a suite of tools that are appropriately tailored to the problem. The Analytical DM factors in assets, systems, networks, processes, and capabilities that are significant to the core elements, i.e., threat, vulnerability, and consequence. The NIPP suggests the assessment be specific to a sector or region.
Intuitive DM	The Intuitive DM may identify with an element of the Assess Risk Component that may necessitate immediate action, and that could transition directly into the Implement Protective Programs Component.
Capability Based DM	The elements of assessing risk will drive Capability Based DM. Threat, vulnerability, and consequence are all linked to the MAs and TCs discussed in Chapter II. Capability Based DM will rely on the risk assessment and analysis for those MAs and TCs that will have the greatest impact in driving down risk.

Prioritize

The NIPP risk management framework provides the process for developing comparable estimates of the risk relevant to CI/KR. The framework is applicable to risk assessments on an asset, system, network, function, sector, state, regional, or national basis. The NIPP also suggests that the prioritization process provides information that can be used during incident response to inform decisions regarding issues associated with CI/KR restoration. The NIPP delineates this process into two related activities: The first determines which sectors, regions, or other aggregation of CI/KR assets, systems, networks, or functions are subject to the highest risk as calculated using the NIPP risk management framework. Those exposed to the greatest risk are accorded the highest priority in risk management program development. The second activity determines which protective actions are expected to provide the greatest mitigation of risk for any given investment. The risk management initiatives that result in the greatest risk mitigation for the investment proposed are accorded the highest priority in program design, resource allocation, budgeting, and implementation. This approach ensures that programs make the greatest contribution possible to overall CI/KR risk mitigation in the context of resources available.[100]

The GAO framework utilized an Alternatives Evaluation Component, whereas the NIPP suggests a more prioritized approach. The GAO concept is based more on a decision-making process than the NIPP concept, which is still meant to identify risk as the primary driver for the decision maker. As outlined by the NIPP, this component of the framework makes sense for the decision maker due to the vast problem space associated with homeland security. A prime example is identifying UASI Regions within states. These regions are developed based on the assets, systems, networks, and functions that are most densely populated within a given region of a state. They may also represent a higher risk landscape and require more security approaches. Therefore, prioritization becomes essential for grant funding as well as resource allocation.

[100] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 43.

(NIPP) Prioritize	
Strategic DM	The Strategic DM can find great utility in implementing a prioritization strategy. A primary use of prioritization is to inform resource allocation decisions, such as where protection programs should be instituted. The Strategic DM may also rely on the risk assessment process so that empirical information can generate a strategy for prioritizing resources. This component is a very strategic-oriented phase within the NIPP framework for preparedness planning.
Operational DM	Based on what the Strategic DM deems to be a prioritized asset, system, network, or function, the Operational DM can acclimate to the components that would lead to the implementation of protective programs.
Tactical DM	The Tactical DM determines what tactical requirements may be needed for a response to a prioritized asset, system, network, or function. An example would be tactical teams deployed within a chemical facility that would require proper PPE.
Analytical DM	The Analytical DM can identify or develop a suite of tools that are tailored for prioritized assets, systems, networks, or functions. For example, the Analytical DM would not use the same vulnerability assessment tool for stadiums as it would for dams due to the different methods of a potential attack.
Intuitive DM	The Intuitive DM may use intelligence products, and may chose to vary prioritization, based on the reliability of those products.
Capability Based DM	The Capability Based DM may determine which capabilities are necessary for protective actions against multiple threat scenarios that target prioritized assets, systems, networks, and functions. By building a sustainable capacity of capabilities, risk can be driven down for prioritized CI/KR.

Implement Protective Programs

According to the NIPP, the nation's CI/KR is widely distributed in both a physical and a logical sense. Effective CI/KR protection requires both distributed implementation of protective programs by security partners and focused national leadership to ensure implementation of a comprehensive, coordinated, and cost-effective approach. At the implementation level, protective programs consist of diverse actions undertaken by various security partners. From the leadership perspective, programs are structured to address coordination and cost-effectiveness.[101]

The NIPP describes protective actions involving measures designed to prevent, deter, and mitigate the threat, to reduce vulnerability to an attack or other disaster, to minimize consequences, and to enable timely, efficient response and restoration in a post-

[101] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 45.

event situation. There is great necessity in the protective actions that represent the core elements for this component of the framework. The GAO implies that during the implementation and monitoring phase, preparedness actions should be implemented. This component of the NIPP acknowledges that protective actions reduce risk by addressing each of the risk assessment elements of threat, vulnerability, and consequence. The protective actions described below vary across a spectrum of activities, but are of great value to the decision maker:

- **Deter:** Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable. Examples include improved awareness and security (e.g., restricted access, vehicle checkpoints) and enhanced police and/or security officer presence;
- **Devalue:** Reduce the attacker's incentive by reducing the target's value. Examples include developing redundancies and maintaining backup systems or key personnel;
- **Detect:** Identify potential attacks and validate and/or communicate the information, as appropriate. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, network monitoring systems, operation alarms, surveillance, detection and reporting, and employee security-awareness programs;
- **Defend:** Protect assets by preventing or delaying the actual attack, or reducing an attack's effect on an asset, system, or network. Examples include perimeter hardening by enhancing buffer zones, fencing, structural integrity, and cyber defense tools such as antivirus software.[102]

In addition to the protective actions, the NIPP suggests that protective programs should focus on the overall preparedness aspects for reducing risk. These programs can link the necessary actions that would benefit the decision maker when faced with a critical incident. The following preparedness functions are built into driving down risk, and are linked to the actions by decision makers throughout various levels of the framework.

- **Mitigate:** Lessen the potential impact of an attack, natural disaster, or accident by introducing system redundancy and resiliency, reducing asset dependency, or isolating downstream assets;

[102] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 45.

- **Respond:** Activities designed to enable rapid reaction and emergency response to an incident, such as conducting exercises and having adequate crisis response plans, training, and equipment;
- **Recover:** Allow businesses and government organizations to resume operations quickly and efficiently, such as using comprehensive mission and business continuity plans that have been developed through prior planning.[103]
-

(NIPP) Implement Protective Programs	
Strategic DM	The Strategic DM can develop a preparedness strategy or a situational COA by ensuring that the Implementation of Protective Programs Component is compatible to the asset, system, network, function, sector, or region.
Operational DM	The Operational DM can utilize the protective actions of deterrence, detection and defense to support a COA that is specific to an asset, network, system, or function, sector, or region. Based on threat, intent and capability, the Operational DM can ensure the adequate protective actions are employed.
Tactical DM	The Tactical DM can focus on the threat, capability, and intent, and ensure that the operational protective actions are executed. The Tactical DM may also rely on an intuitive COA, if necessary.
Analytical DM	The Analytical DM can support the preparedness strategy by supporting the Strategic, Operational, and Tactical DMs with adequate analysis and assessment that is tailored to the protective actions.
Intuitive DM	The Intuitive DM is vital during the execution phase for this component of the framework. Protective actions may be dynamic and require Intuitive DM to defeat a given threat or attack.
Capability Based DM	Protective programs are based on capabilities. Capability Based DM supports every aspect of the protective actions and preparedness functions.

Measure Effectiveness

According to the NIPP, the Measuring Effectiveness Component drives continuous improvement of CI/KR risk-mitigation programs at the sector level and overall program performance at the national level. The NIPP uses a metrics-based system to provide feedback on efforts to attain the goal, as well as supporting objectives. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met, or to articulate gaps in the national effort or supporting sector efforts. The assessment enables the identification of corrective actions, and provides

[103] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 47.

decision makers with a feedback mechanism to help them make appropriate adjustments. It can also provide qualitative insights to help make informed decisions. Cost-benefit analyses of programs, lessons learned from exercises, actual incidents, and alerts provide additional objective input into the process.[104]

(NIPP) Measure Effectiveness	
Strategic DM	The Strategic DM can utilize the Measure Effectiveness Component to ascertain whether the components and other elements of the framework are enhancing homeland security preparedness strategies.
Operational DM	The Operational DM can utilize the elements of the Measure Effectiveness Component through exercises, lessons learned, and actual incidents in order to enhance qualitative insights to make better informed decisions for an identified COA.
Tactical DM	The Tactical DM can also utilize the elements of the Measure Effectiveness Component through exercises, lessons learned, and actual incidents in order to enhance qualitative insights to make better informed decisions for an identified COA that requires action and execution.
Analytical DM	The Analytical DM can utilize the metrics that offer a quantitative assessment to affirm that specific objectives are being met, or to articulate gaps in the state/region effort or supporting sector efforts.
Intuitive DM	The NIPP's description of the Measure Effectiveness Component adds to the experience and improves pattern recognition based on the knowledge that the Intuitive DM can gain through exercises, lessons learned, and actual incidents.
Capability Based DM	Capabilities are measured and evaluated during exercises and actual incidents. The Capability Based DM can utilize the aspects of the Measure Effectiveness Component to ascertain various levels of capabilities through scenario enhancements.

The NIPP framework is clearly articulated in the text from the National Infrastructure Plan (NIP). This makes it easier to define the core elements within each component of the framework. From the decision maker's perspective, the definitive elements are what surfaced throughout the analysis of the framework. From these elements, the principal decision-making process interpreted the value for that particular component.

The feedback loop illustrated at the conclusion of the Measure Effectiveness Component suggests that components of the framework are dependent upon one another. This dependency allows the framework to be fluid, and presents a step-by-step approach for the decision maker to follow. Central to the framework is the Assess Risk

[104] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* 2006, 48.

Component. This component produced the elements of threat, vulnerability, and consequences. An essential theme to this paper, and as was defined as a focal point for terrorism risk, are these three elements. The Assessment of Risk Component generated elements reflective of baseline criteria and tool enhancements for risk assessment methodologies. Although there are discrepancies in how effective these tools have been, the NIP document acknowledges that risk assessment tools are required for decision makers to make better-informed decisions.

4. The International Risk Governance Council (IRGC) Framework

Ortwin Renn, the creator and author of a white paper on the IRGC Risk Governance Framework, describes it as "an integrated analytic framework for risk governance which provides guidance for the development of comprehensive assessment and management strategies to cope with risks, in particular at the global level.[105] Renn and the IRGC chose to use the term "risk governance" with the intention of representing the many different groups in society, from governments to individuals — who collectively make decisions. These principles underpin IRGC's view that risk governance includes the actors, rules, conventions, processes, and mechanisms concerned with how relative risk information is collected, analyzed, and communicated, and how management decisions are taken.[106] Ross asserts that the IRGC chose the term "risk governance" due to the varying several schools of thought on the proper definitions and hierarchical relationship between the terms "risk assessment," "risk analysis," and "risk management." In Ross's analysis of the IRGC Risk Governance Framework, he finds utility in the term "governance" and combines it with the principles of risk management, thus creating "risk management/governance." [107]

[105] Renn, "White Paper on Risk Governance: Towards an Integrative Framework," 11.

[106] Renn and Katherine D. Walker, *Global Risk Governance: Concept and Practice Using the IRGC Framework.* (Berlin, Germany: Springer Publishing, 2008). Xxvi.

[107] Robert Ross, "Risk and Decision Making in Homeland Security," Attachment B.

The IRGC framework offers a much more comprehensive approach than both the GAO and NIPP, but has yet to be utilized within the security studies field.[108] The framework's process for dealing with risk comprises five phases: pre-assessment; risk appraisal, risk characterization/evaluation; risk management; and risk communication (Figure 9). The framework also distinguishes between a management sphere (containing decision making and implementation) and an assessment sphere (containing risk appraisal). The pre-assessment, characterization/evaluation and communication phases are in both spheres because, although the IRGC strongly endorses the separation of risk appraisal and management, these three other phases need the combined efforts of the people responsible for both. The IRGC positions risk communication at the center of the framework to reflect its crucial role throughout — rather than at a particular point of — the entire process. The IRGC framework is, therefore, deliberately open, interlinked, and iterative.[109]

[108] In a received email from the author Ortwin Renn, he encourages the use of the IRGC framework for due to the generic principles that are well suited to deal with a large variety of risks including security issues.

[109] Renn and Walker, *Global Risk Governance.*

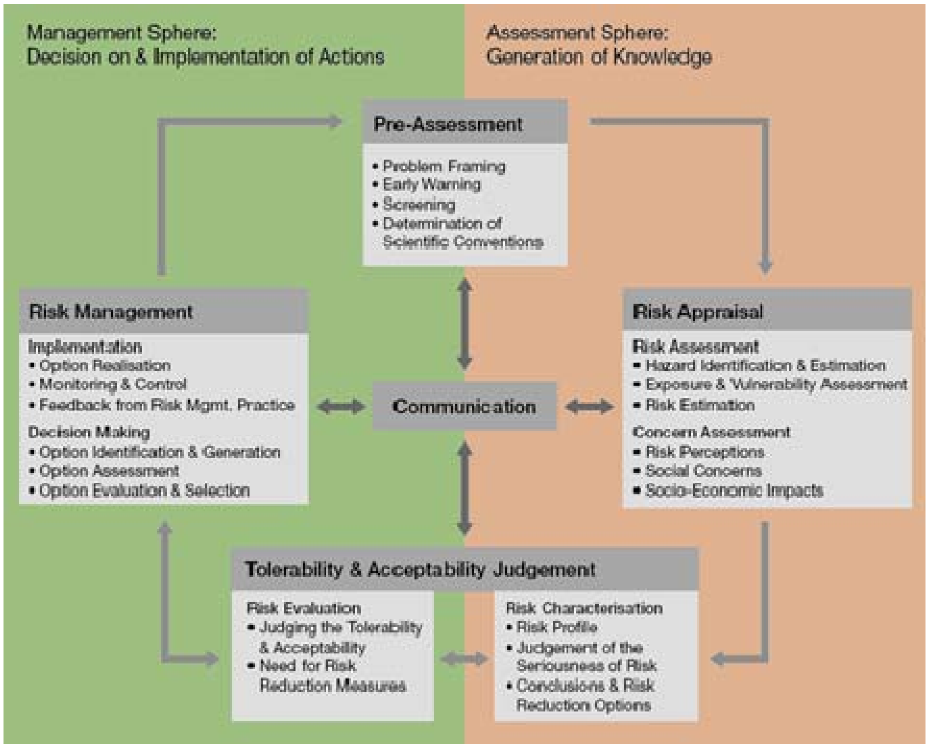

Management Sphere:
Decision on & Implementation of Actions
Assessment Sphere:
Generation of Knowledge
Pre-Assessment
• Problem Framing
• Early Warning
• Screening
• Determination of Scientific Conventions
Risk Management
Implementation
• Option Realisation
• Monitoring & Control
• Feedback from Risk Mgmt. Practice
Decision Making
• Option Identification & Generation
• Option Assessment
• Option Evaluation & Selection
Communication
Risk Appraisal
Risk Assessment
• Hazard Identification & Estimation
• Exposure & Vulnerability Assessment
• Risk Estimation
Concern Assessment
• Risk Perceptions
• Social Concerns
• Socio-Economic Impacts
Tolerability & Acceptability Judgement
Risk Evaluation
• Judging the Tolerability & Acceptability
• Need for Risk Reduction Measures
Risk Characterisation
• Risk Profile
• Judgement of the Seriousness of Risk
• Conclusions & Risk Reduction Options

Figure 9. IRGC Risk Governance Framework Core Process[110]

The IRGC framework is very comprehensive and offers a different view of how risk can be managed through the utility of a governing framework. Ross suggests that a particular advantage of the IRGC Core Process is the distinction drawn between the Assessment and Management Spheres.[111] This distinction makes the IRGC framework unique; however, it does acknowledge that certain components need the combined efforts of people representing both the Management and Assessment Spheres. The analysis for this framework will be consistent with the two spheres. Rather than utilize the principal decision-making processes for each component, we will delineate this process into the Assessment Sphere: Generation of Knowledge, and the Management Sphere: Decision on and Implementation of Actions. As suggested by the IRGC, the pre-assessment, characterization/evaluation and communication phases are in both spheres, and will be acknowledged through the principal decision-making processes.

[110] Renn, “White Paper on Risk Governance: Towards an Integrative Framework,” 13.

[111] Robert Ross, “Risk and Decision Making in Homeland Security,” Attachment B.

Pre-Assessment

- Problem Framing
- Early Warning and Monitoring
- Screening

The purpose of the Pre-Assessment Phase is to capture both the variety of issues that stakeholders and society may associate with a certain risk, as well as existing indicators, routines, and conventions that may prematurely narrow down, or act as a filter for, what is going to be addressed as risk.[112] The IRGC suggests that these preliminary thoughts provide a systematic review of risk-related actions that must begin with an analysis. This first element of the Pre-Assessment Phase is referred to as problem framing, which essentially assists in identifying the source of the threat. From a homeland security perspective, problem framing can include a host of risks, stemming from terrorism to natural disasters. Problem framing can also assist in the decision-making process by narrowing the scope of the risk to a specific act of terrorism targeting an identified sector.

A second element of the Pre-Assessment Phase is early warning and monitoring. This element is intended to support observations and indicators of potentially damaging events or their precursors by monitoring the environment for signals of risk.[113] Early warning and monitoring is a prime example of what is expected of the U.S. intelligence community. Figure 5B in Chapter II illustrates intelligence-collection disciplines. The intelligence community, through these various disciplines, is constantly implementing the element of early warning and monitoring.

The third element of the Pre-Assessment Phase is referred to as *screening*. Screening is the process of sifting and selecting information about risk in order to allocate the risk to a particular category or to a particular control regimen.[114] As the final element of this phase, screening captures the essence of what has been framed as a risk problem and what has been monitored as a risk. An example would be the framed risk problem space associated with passenger rail transportation, screened for multiple attacks within an identified jurisdiction.

[112] Renn, “White Paper on Risk Governance: Towards an Integrative Framework.”

[113] Ibid., 24.

[114] Ibid., 25.

Risk Appraisal

- Risk Assessment
- Concern Assessment

The process of the Risk Appraisal Phase brings together the information necessary for risk characterization, evaluation, and management. This includes not just the results of scientific risk assessment, but also information about risk perceptions and economic and social implications of the risk consequence.[115]

The IRGC framework opts to use the Risk Appraisal Phase as its primary component for the Assessment Sphere, which captures the Risk Assessment and Concern Assessment elements. The IRGC envisions the Risk Appraisal Phase as having two process stages: First, natural and technical scientists use their skills to produce the best estimate of the physical harm that a risk source may induce (this is referred throughout the white paper as risk assessment). Second, social scientists and economists identify and analyze the issues that individuals or society as a whole link with a certain risk (referred to as concern assessment).[116]

Risk Assessment: The purpose of risk assessment is the generation of knowledge linking specific risk agents, such as terrorism or natural disaster, with uncertain but possible consequences. The final product of risk assessment is an estimation of the risk in terms of a probability distribution of the modeled consequences. The different stages of risk assessment vary from risk source to risk source.[117] The IRGC also recognizes that there have been many efforts to produce a harmonized set of terms that would cover a wide range of risks and risk domains. This was noted previously in this paper, regarding the utility of a common lexicon within the risk domain. The IRGC suggests, however, that there is agreement on basically three core components of risk assessment:

- An identified and, if possible, estimation of the hazard;
- An assessment of exposure and/or vulnerability;

[115] Renn, "White Paper on Risk Governance: Towards an Integrative Framework," 79.

[116] Ibid., 34.

[117] Ibid., 27.

- An estimation of risk, combining the likelihood and the severity of the targeted consequences based on identified hazardous characteristics and the exposure/vulnerability assessment.[118]

The IRGC chose to use very generalized terms that could be applied to a large range of issues regarding risk. The term *hazard* would mirror what has been referred to as *threat* throughout this paper. It further acknowledges that the basis of risk assessment is the systematic use of analytical, largely probability-based methodologies. Yet these methodologies require a great deal of quantitative analysis and statistical data, which could be difficult to collect. This is the problem with trying to determine threat. We know it exists. We know intent and capability are linked to it. But, unless intelligence collectors can identify the threat, we cannot measure it.

Earlier in this paper, references were made to the complexity and uncertainty associated with risk as it pertains to the homeland security problem space. The IRGC suggests that these two terms challenge the risk assessment process. It suggests that complexity refers to the difficulty of identifying and quantifying casual links between a multitude of potential causal agents and specific, observed facts.[119] An example of complexity within the homeland security domain would be the protection of critical infrastructure. The U.S. infrastructure is extremely large and complex. This complexity is compounded further when combined with the interdependencies and collateral impacts that one can have on another. What should be protected? How should it be protected, and at what cost?

The IRGC asserts that it is essential to acknowledge, in the context of risk assessment, that human knowledge is always incomplete and selective, and thus contingent on uncertain assumptions, assertions, and predictions.[120] In this context, the uncertainty of risk assessment can be linked to the intelligence collection and dissemination process. If one assumes that a piece of threat-based intelligence is critical

[118] Renn, "White Paper on Risk Governance: Towards an Integrative Framework," 27.

[119] Ibid., 29.

[120] Ibid., 30.

— but that it is uncertain whether it is indicative of an attack — are immediate preventive and protection actions called for, or should the situation be monitored while intelligence analysts wait for more information?

The IRGC acknowledges that complexity and uncertainty exist when risk assessment is being applied to a particular issue or problem, especially when probabilistic risk assessment methodologies cannot be applied. These elements of the risk assessment component can improve the decision-making process when not all variables are visible, especially at the intuitive decision-making stage.

Concern Assessment: Concern assessment extends beyond the scientific process of risk assessment. This concept relates to the concerns of social and economic implications of risk. What is the public's perception of how risk is being managed?[121] Decision makers need a better understanding of how the public perceives risk in general, and specific risks associated with terrorism. Risk management decisions may be influenced by public perceptions of risk, which may result in a shift of resource allocation or operational deployment strategies. Part B of Chapter IV is dedicated to risk perception and the passenger rail threat. It captures the social element that is intrinsic to the terrorism threat, and reflects the element of concern assessment.

Tolerability & Acceptability Judgment

- Risk Characterization
- Risk Evaluation

The IRGC refers to this component of the framework as being the most controversial phase for handling risk. Risk characterization and evaluation judges a risk's acceptability and/or tolerability. A risk deemed "acceptable" is usually limited in terms of negative consequences, so that it is taken on without risk reduction or mitigation measures being implemented. A risk deemed "tolerable" links the undertaking of an activity, one that is considered worthwhile for the value-added benefit it provides, with specific measures to diminish and limit the likely adverse consequences.[122]

[121] Renn, "White Paper on Risk Governance: Towards an Integrative Framework," 34.

[122] Ibid., 36.

The IRGC emphasizes that the Tolerability and Acceptability Judgment Phase also sits in the center of the framework, adding value to both the Assessment and Management Spheres. While risk characterization compiles scientific evidence based on the results from the risk appraisal, risk evaluation assesses broader, value-based issues that also influence judgment, which is an inherent element of the risk management phase.

Risk Management

- Implementation
- Decision Making

The IRGC asserts that the risk management phase starts with a review of all relevant information, in particular that from the combined risk appraisal, consisting of both a risk assessment and concern assessment, whereby the latter is based on risk perception studies, economic impact assessments, and the scientific characterization of social responses to the risk source. This information, together with the judgments made in the phase of risk characterization and evaluation, form the input material on which risk management options are assessed, evaluated and selected.[123]

This component of the IRGC framework represents the implementation and decision-making elements. Essential to these two elements is what the IRGC refers to as an assessment of risk management options. Each of these options is intended to be related to the reduction of risk, and to assist in the decision-making process:

- Effectiveness
- Efficiency
- Minimization of external side effects
- Sustainability
- Fairness
- Political and legal implementation
- Ethical acceptability
- Public acceptance

[123] Renn, “White Paper on Risk Governance: Towards an Integrative Framework,” 14.

It is the task of the risk management decision maker to ensure that each of these options is evaluated, selected, implemented, and monitored for effectiveness. These steps mirror a decision-making process, and are offered by the IRGC as an essential element for the risk management component of the framework. A primary theme throughout this paper, however, has been that decision making is being implemented at every phase of the risk management framework and for each component. This suggests that, although the IRGC recognizes decision making is a core process for risk management, it is also necessary throughout the entire framework.

Communication

The remaining element of the IRGC framework is risk communication, which is of major importance throughout the entire risk-handling chain. Risk communication should enable stakeholders and civil society to understand the rationale of the results and decisions, from the risk appraisal and risk management phases, when they are not formally part of the process. Risk communication should also help them to make informed choices about risk, balancing factual knowledge about risk with personal interests, concerns, beliefs, and resources, when they are involved in risk-related decision making.[124]

Ross acknowledges the utility of communication, and states,

> government efforts to manage societal risks must be acceptable to the majority of those making up the society or the government will fail. This again points out the importance of communication. Risk Communication is not limited to those involved in the Framework's Core Process. Rather, Risk Communication must extend to a society as a whole.[125]

Figure 10 illustrates risk communication extending beyond the interior components of the core process to society as whole.

[124] Renn, "White Paper on Risk Governance: Towards an Integrative Framework," 15.

[125] Robert Ross, "Risk and Decision Making in Homeland Security," Attachment B.

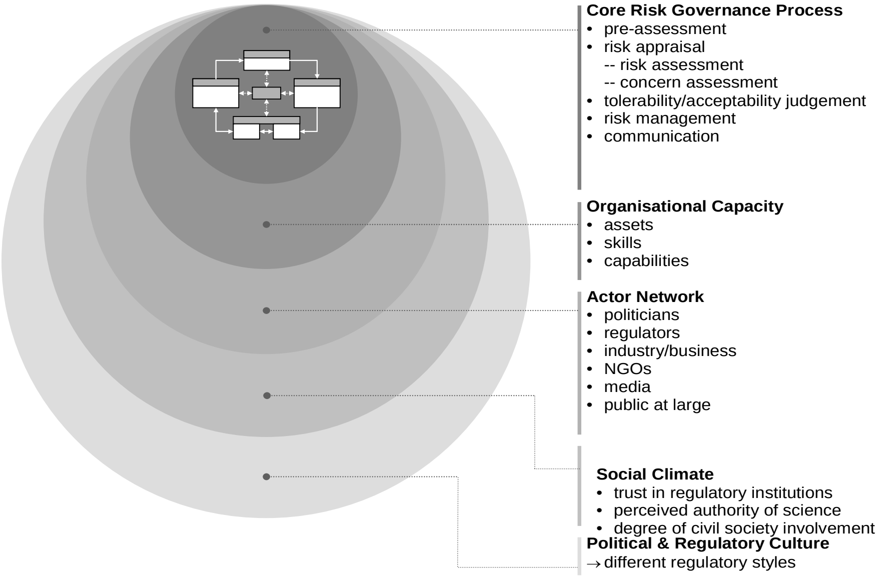


Figure 10. The IRGC Risk Governance Framework Macro Context[126]

(IRGC) Assessment Sphere	
Strategic DM	The Assessment Sphere can support the Strategic DM with developing goals and objectives through the combination of the Pre-Assessment and Risk Appraisal Components. The Strategic DM can proceed with a strategic COA due to the inherent elements of each component that contains problem framing, risk assessment, and concern assessment.
Operational DM	The Operational DM can utilize the Pre-Assessment and Risk Appraisal Components in an effort to make better-informed decisions that reflect early warning and screening and risk assessment. The risk assessment offers identified hazards and vulnerabilities from which the Operational DM can draw.
Tactical DM	The Assessment Sphere supports the Tactical DM through the Risk Assessment Component that identifies adversarial intent and capabilities.
Analytical DM	The Analytical DM can utilize each component of the Assessment Sphere due to the Communication Component that supports the connectivity of the IRGC framework. The Analytical DM can even cross over into the Risk Management Phase due to this supporting feature. The Analytical DM can utilize the risk characterization and evaluation to determine if the risk is acceptable or tolerable.
Intuitive DM	The Assessment Sphere offers insight into complexity and uncertainty. These are elements of the risk assessment component that are referred to as unclear variables of risk. The Intuitive DM can be reactionary, and rely on knowledge and experience if faced with a complex, uncertain problem. The Intuitive DM may rely on the risk evaluation to assess a broader aspect of risk that requires knowledge and experience.
Capability Based DM	The Pre-Assessment and Risk Appraisal Components can support the Capability Based DM to make better informed decisions by identifying the hazards and vulnerabilities associated with risk assessment and the early warning and screening elements of pre-assessment.

[126] Robert Ross, “Risk and Decision Making in Homeland Security,” Attachment B.

(IRGC) Management Sphere	
Strategic DM	The Management Sphere is designed to support Implementation and Decision-making Phases. The Strategic DM can find support in the Management Sphere throughout the entirety of the framework due to the Communication Component.
Operational DM	The Operational DM will rely on the Management Sphere for implementation, monitoring, and effectiveness for a COA.
Tactical DM	The Tactical DM will rely on the Management Sphere for implementation, monitoring, and effectiveness for a COA.
Analytical DM	As is the case for the Analytical DM in utilizing the Assessment Sphere, the same can be said for the Management Sphere. The Analytical DM can find utility in the Communication Component that supports both components of the framework.
Intuitive DM	The Management Sphere is supportive of implementation, monitoring, and effectiveness. The Intuitive DM is directly engaged in this phase of the framework in the event of an immediate change in COA. Complexity and uncertainty engage the Intuitive DM throughout the Management Sphere as well.
Capability Based DM	The Capability Based DM factors into the implementation, monitoring, and effectiveness elements due to the overarching support for the strategic, operational, and tactical decision makers.

B. AN INTEGRATIVE RISK MANAGEMENT/GOVERNANCE FRAMEWORK

1. Introduction

This segment of the chapter will identify the commonalities and quality attributes that exist in each of the risk management frameworks. Based on the analysis of each framework, the essential components and core elements will be extracted and integrated into a risk management/governance framework. The risk management/governance framework is derived from the relative impact that each component and its core elements had on the principal decision-making processes. Of each of the frameworks, the IRGC model supports the application of a communication component that is meant to interconnect principles of risk, even though they are categorized as risk management or risk assessment principles. Communication is central to the core process, illustrating connectivity among all components.

An additional feature evident in the IRGC framework acknowledges the fact that combined efforts of decision makers may overlap into risk management and risk assessment-related disciplines. This is reflected in the Management and Assessment Spheres. These two attributes will provide the structure for the risk management/governance framework. Figure 11 illustrates the Integrative Risk Management/Governance Framework that is further explained in the remainder of this chapter.

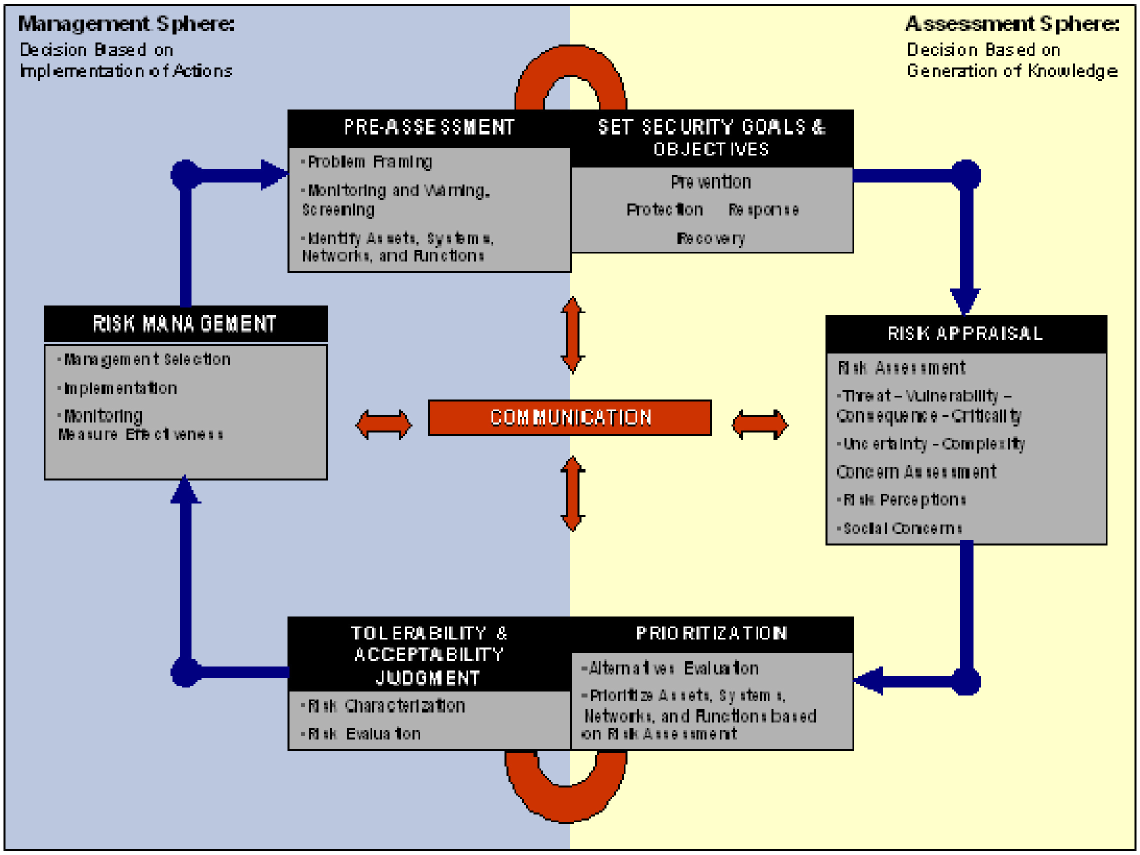


Figure 11. Integrative Risk Management/Governance Framework

2. Identified Commonalities and Quality Attributes for a Risk Management/Governance Framework

Pre-Assessment

- **Problem Framing**
- **Monitoring and Warning, Screening**
- **Identify Assets, Systems, Networks, and Functions**

A common component of the GAO and NIPP frameworks is the utility of defining strategic goals and objectives for a given homeland security issue or problem. The IRGC, however, offers a Pre-Assessment Component to support the decision maker in developing a strategy that identifies the source of the risk or threat. By identifying the assets, systems, networks, and functions, which are core elements of the NIPP framework, problem framing, monitoring and warning, and screening can be applied to assess the criticality and threat to these elements. Based on this assessment, the decision maker can proceed with developing security goals and objectives for a specified sector or region that contains these elements.

Set Security Goals & Objectives

- **Prevention**
- **Response**
- **Protection**
- **Recovery**

Both the GAO and NIPP frameworks initiated the risk management process by setting security goals and objectives. This component was evident and essential for the strategic decision maker. The NIPP component referred to definitive prevention, protection, response, and recovery postures that security partners seek to attain. The elements of setting security goals and objectives in combination with the elements of the pre-assessment phase can support the decision maker in developing goals and objectives that are focused on prevention, protection, response, and recovery. Each identified asset, system, network, or function can be linked to each of these mission capabilities for a specified sector or region.

The Integrative Risk Management/Governance Framework illustrates the pre-assessment, and setting security goals and objectives as a starting point for the risk management/governance process. The framework acknowledges that both components are interconnected and influence decision making through both risk management and risk assessment principles. For example, in the case of a threat to passenger rail systems for a given region, the pre-assessment/security goals and objectives components will rely on principles relative to the Management Sphere in order to implement proper deployment and monitoring procedures. The principles associated with the Assessment Sphere can assist in identifying proper analysis tools and systems that support problem framing, and monitoring and warning. As a result of this interconnectivity between both risk spheres, the decision maker can develop the most adequate course of action that is reflective of the goals and objectives.

Risk Appraisal

Risk Assessment

- **Threat – Vulnerability – Consequence - Criticality**
- **Uncertainty - Complexity**

Concern Assessment

- **Risk Perceptions**
- **Social Concerns**

The Risk Appraisal Component is a combination of risk assessment and concern assessment, which are core components of the IRGC framework. Essential to this component are the elements of threat, vulnerability, and consequence. Criticality, a GAO element, has been added to this trio. Each of the principal decision-making processes reflect a great deal of reliability on the elements of the risk assessment component throughout each of the frameworks. The risk assessment component in the GAO framework was central to the model, and factored into each of the principal decision-making processes throughout the cycle. The NIPP framework continually referred back to the core elements of threat, vulnerability, and consequence for each phase. The NIPP dissected each of these elements, and explained the attributes and enhancements that the decision maker could adopt. The NIPP also refers to analysis tools and systems that can support risk assessment methodologies. The decision-making processes reflected the need for tools that are developed using proven methodologies, and that are appropriately tailored for a problem or issue.

The terms *uncertainty* and *complexity* were described in the risk assessment phase for the IRGC framework. Intuitive decision making is essential when faced with issues that are uncertain and complex. The IRGC acknowledges that complexity and uncertainty exist when risk assessment is applied to a particular issue or problem, especially when probabilistic risk assessment methodologies cannot be applied. Uncertainty and complexity reverberate throughout the homeland security problem space. Therefore, it is critical that tools and assessment methodologies are tailored for each of the elements, and are applied to identified assets, systems, networks, and functions for a specific sector or region. This enables the decision maker to make the best-informed decision for a given problem.

Concern Assessment extends beyond the scientific process of risk assessment, and engages the decision maker with concerns associated with social and public perceptions of risk. Concern Assessment takes into account what the decision maker may not deem to be critical, but that may be perceived differently in the eyes of the public. For example, the media may report an apparent terrorist threat against the NYC subway system. The risk assessment, however, in conjunction with the threat analysis, may conclude that there is no credible threat. Protection measures may be employed as a reactionary course of action to mitigate the public's perception of terrorism risk.

Prioritization

- **Alternatives Evaluation**
- **Prioritize Assets, Systems, Networks, and Functions based on Risk Assessment**

The NIPP framework prioritizes assets, systems, networks, and functions based on the risk assessment. The GAO framework implements an Alternatives Evaluation component, implying that, while decision making is based on the risk assessment, it can divert if there is a change in strategy. The Prioritization Component provides information that can be used during the employment of prevention, protection, and response issues that can help inform decision makers. Each of the principal decision-making processes found utility in the Prioritization Component that generally led to the implementation phase.

Prioritization is placed at the lower half of the Assessment Sphere for this framework so that the decision maker can take into account all relative assessment information that is generated through the Pre-Assessment, Security Goals and Objectives, and Risk Appraisal Components. This is integral to the process prior to risk characterization and evaluation, which is aimed at judging a risk’s acceptability and/or tolerability.

Tolerability & Acceptability Judgment

- **Risk Characterization**
- **Risk Evaluation**

The Tolerability and Acceptability Judgment Component is linked with the Prioritization Component. This is meant to illustrate a seamless transition into the Management Sphere. Risk characterization and evaluation revealed that they both have utility for analytical and intuitive decision making. Prior to implementation, this component can assist the decision maker in moving forward with management selection, monitoring, and measuring effectiveness.

Risk Management

- **Management Selection**
- **Implementation**
- **Monitoring Measure Effectiveness**
- **Option Identification**

Throughout this paper, risk management has been defined as the overarching principle responsible for decision making and driving down risk. Each framework reflects a combination of risk principles that are meant to drive the decision-making process. The GAO framework illustrated a decision-making process and included risk assessment as a component. The NIPP also reflected a decision-making process, but detailed the elements of each component. In both frameworks, the principal decision-making process found utility in the final phase of the process. The IRGC includes risk management as a component of its core process, illustrating that risk management and risk assessment integrate with one another throughout the process.

This component of the risk management/governance framework is assembled to illustrate the utility of combining the final components of the GAO and NIPP frameworks — management selection, implementation, monitoring, and measuring effectiveness — into the Risk Management Phase. With communication as a central component to the process, risk management and risk assessment can support one another.

IV. PASSENGER RAIL TRANSPORTATION RISK PROBLEM SPACE

A. OVERVIEW OF THE PASSENGER RAIL TRANSPORTATION SECTOR THREAT

1. Introduction

In its historic report, the 9/11 Commission stated,

> While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime surface transportation. Initiatives to secure shipping containers have just begun. Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive.
>
> The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost effective ways of doing so, and then develop a plan, budget, and funding to implement the effort."[127]

The Transportation Security Administration (TSA) has responded to the recommendations made by the 9/11 Commission, and has taken significant steps to improve security for the transportation sector. TSA has adopted a risk-management approach to guide decisions, and to maximize resources where they are most needed. The TSA has undertaken numerous initiatives to strengthen transportation security, particularly in aviation.[128] Secured cockpit doors, the Federal Flight Deck Officer Program, and a vastly expanded Federal Air Marshal Program have reduced the risk of attacks similar to those of September 11.[129]

[127] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* 391.

[128] Government Accountability Office, *Transportation Security – Systematic Planning Needed to Optimize Resources,* Washington, DC: Government Accountability Office, 2005, 1.

[129] Transportation Security Administration. *Risk Management.* http://www.tsa.gov/approach/risk/index.shtm (Accessed October 18, 2007).

The nation's transportation sector is a vast, interconnected network of diverse modes. In addition to aviation, key modes of transportation include highways, motor carrier (trucking), motor coach (intercity bus), maritime, pipeline, rail (passenger and freight), and transit (buses, subways, ferry boats, and light rail).[130] Given this vast transportation network, quick and easy access for passengers and cargo must be maintained while identifying the best possible strategies for security. In recent years, the most devastating terror attacks have been against passenger rail infrastructure. Rail infrastructure continues to be targeted on a transnational front, resulting in mass casualties and widespread disruption. The London and Madrid bombings opened the eyes of homeland security practitioners as to the devastation and possibilities of similar attacks targeting America's transportation systems. An attack on passenger rail serves the chief objectives of many terrorists, which are to cause mass casualties, impact economic vitality, and create fear.

This global trend of attacking rail transportation may be a shift and adaptation in terrorist tactics and modus operandi. Bruce Hoffman states,

> Terrorism is perhaps best viewed as the archetypal shark in the water. It must constantly move forward to survive and indeed to succeed. Although survival entails obviating the governmental countermeasures designed to unearth and destroy the terrorists and their organization, success is dependent on overcoming the defenses and physical security barriers designed to thwart attack. In these respects, the necessity for change in order to stay one step ahead of the counterterrorism curve compels terrorists to change — adjusting and adapting their tactics and modus operandi, and sometimes even their weapon systems as needed. [131]

The methodology for including Hoffman's research in this study is to illustrate the benefit of conducting a qualitative threat analysis central to one area of the vast homeland security problem space. By narrowing the scope of threat, vulnerability, and consequence to a specific sector and region, we can better evaluate the utility of an integrative risk management/governance framework for homeland security decision making. Three

[130] Government Accountability Office, *Transportation,* 3.

[131] Bruce Hoffman, *"Inside Terrorism"* (London: Orion and New York: Columbia University Press, 1998), 180-183.

underlying threat-analysis factors have been identified that are central to the passenger rail transportation sector: global attacks and threats to passenger rail transit systems; the terror threat to passenger rail transportation for New York and New Jersey; and analysis and key judgments of the New York/New Jersey passenger rail system.

2. Global Attacks and Threats to Passenger Rail Transit Systems

High profile terrorist attacks on rail systems in Madrid, London, and Mumbai illustrate that the U.S. public transportation system also is a vulnerable target. The abundance of passengers, combined with the need for easy access, makes securing passenger railways a daunting task. In his remarks before the U.S. Senate Committee, TSA Administrator Kip Hawley stressed that TSA must keep its focus on the highest priority items, which are informed and driven by the current threat environment.[132] He further stated that the National Intelligence Estimate indicated that, over the next three years, the threat will continue, with terrorists attempting transportation sector attacks on a grand scale.[133]

Although there have been indications of terrorist threats against U.S. passenger rail transportation systems, the majority of attacks have been executed abroad. These five high profile terrorist attacks were committed against passenger rail systems, resulting in multiple casualties and large-scale destruction.

a. Moscow, Russia Metro Bombing – February 6, 2004

Overview: A blast tore apart a metro train car in Moscow during the morning rush hour on February 6, 2004. The train was traveling between the Paveletskaya Station and the Avtozavodskaya Station around 8:40 a.m. The explosion occurred in the second car of the train, blowing out windows and hurtling metal pieces of the train in all directions. The device had an explosive power of about four to five kilograms of TNT. The device was similar to that used in the commuter train attack in

[132] Kip Hawley, *"Implementing Recommendations of the 9/11 Commission Act of 2007"* testimony before the U.S. Senate Committee, http://www.tsa.gov/press/speeches/101607_hawley.shtm (Accessed on October 24, 2007).

[133] Ibid.

Yessentuki in 2003, which was also constructed with large quantities of TNT. Those who survived were forced to walk through the dark tunnel to exit the subway. Forty people were killed and 122 injured.[134]

Terrorist Group: Russian officials believe that Chechen rebels were behind the attack, particularly terrorists affiliated with Abu al-Walid al-Ghalidi.[135]

Tactic: The main theory of investigators was that the blast was perpetrated by two female suicide bombers.[136]

b. Madrid, Spain Train Bombings – March 11, 2004

Overview: 191 people were killed and more than six hundred injured when ten bombs detonated in four different locations on Madrid's train line. Three of these bombs detonated in a train that was pulling into the Atocha Station, a busy hub for the commuter train line and the metro rail. The bombs were in backpacks and were detonated by cell phones.[137]

The Madrid attack is unique because it provides a glimpse into an emerging threat known as "home-grown terrorism." According to Daniel Benjamin and Steven Simon, "…the Madrid bombings were not designed, funded, or executed by al Qaeda operatives. They were carried our by Muslim men, none of whom had ever been to an al Qaeda's camp in Afghanistan, and only one of whom had anything that could be called terrorist training."[138] Madrid demonstrated the global reach of an ideology, and showed all too plainly that those who hold these ideas live and work in the West, and that their numbers are growing, as is the danger they pose.[139]

[134] MIPT Terrorism Knowledge Base web site http://www.tkb.org/Incident.jsp?incID=17994 (Accessed October 31, 2007).

[135] Ibid.

[136] Ibid.

[137] Ibid.

[138] Daniel Benjamin and Steven Simon, *The Next Attack: The Failure of the War on Terror and a Strategy for Getting it Right* (New York, NY: Henry Holt & Company, 2005), 6.

[139] Ibid., 7.

Terrorist Group: This group represented an extension of the global network of Jihad.[140] The suspects hailed from Morocco, India, Syria and Spain. In its claim of responsibility, the Abu Hafs al-Masri Brigade says Spain was targeted because of its cooperation with the U.S. war in Iraq. In response to the attacks, the ruling Spanish party was defeated in elections that took place four days after the incident. The incoming prime minister vowed to remove Spanish troops from Iraq.[141]

Tactic: The bombers envisioned that the trains would be both targets and delivery vehicles. Thirteen devices were timed to remotely detonate through the use of cell phones in the stations. The group intended that the concussion from the blast and the hail of glass and metal shrapnel would engulf the morning crowds on the platforms, as well as the passengers still on the trains. Three of the devices failed to detonate.[142, 143]

c. London, England Transit Bombings – July 7, 2005

Overview: The first explosion happened at 8.50 a.m. on eastbound the Circle Line train, No. 204, traveling from Liverpool Street to Aldgate Station. Within one minute, a second explosion took place on Circle Line train No. 216, traveling westbound from Edgware Road to Paddington. A third bomb was detonated approximately two minutes later, on a southbound Piccadilly Line, No. 311. At 9.47 a.m., a fourth bomb was detonated on the top deck of the No. 30 bus at Tavistock Square. Fifty-two people were murdered and seven hundred were injured. Hundreds more were directly affected by the attacks, including passengers who were uninjured but potentially traumatized by the experience.[144] The explosions were carried out by suicide bombers, all of whom died.[145]

[140] Benjamin and Simon, *The Next Attack,* 16.

[141] MIPT Terrorism Knowledge Base web site.

[142] Ibid.

[143] Benjamin and Simon, *The Next Attack,* 4.

[144] London Assembly, *Report of the 7 July Review Committee* (Greater London Authority, June 2006), 12.

[145] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005, Presented to Parliament by the Prime Minister by Command of Her Majesty,* May 2006, 2.

The impact of the London bombing attacks shows that the infrastructure of the rail transportation is vast and vulnerable. Intelligence is critical in preventing such attacks, but oftentimes there simply isn't any intelligence. On July 11, 2005, Prime Minister Tony Blair told Parliament that there was no intelligence specific enough to have prevented the attacks.[146]

Terrorist Group: The July 7 suicide bombers had connections to Pakistan, however, no evidence supported their association with a structured terrorist group.[147] The attacks were an indicator of the rise of Islamist radicalism, which could quite possibly be the greatest challenge in combating acts of terrorism in the West.

Tactics: The bombers' self-detonated satchels contained explosives. The explosive compound used can be made from easily obtainable household ingredients, although experts believe a trained chemist must have assisted the four suicide bombers.[148]

d. Mumbai, India Train Attacks – July 11, 2006

Overview: On July 11, 2006, a series of seven explosions targeted railroad networks in Mumbai. In all, 190 people were killed and 625 were injured. One of the explosions took place in the first-class trains of the Western Railway at Jogeshwari Station.[149] Indian police described the attack as a coordinated terrorist act. Initial police reports indicated the bombs exploded over a six-minute period during the evening rush hour.[150]

[146] *Report into the London Terrorist Attacks on 7 July 2005*, 2.

[147] Ibid., 35.

[148] News Scientist Tech: Explosives Linked to London Bombings Identified, July 15, 2005. Web site http://technology.newscientist.com/article/dn7682 (Accessed on November 3, 2007).

[149] MIPT Terrorism Knowledge Base web site.

[150] Austin Bay, "Real Clear Politics: The Mumbai Terrorist Attack, July 12, 2006," Web site http://www.realclearpolitics.com/articles/2006/07/the_mumbai_terrorist_attack.html (Accessed on October 31, 2007).

Terrorist Group: The Mumbai police accused a lesser-known militant outfit, Lashkar-e-Qahar (LeQ), for carrying out the coordinated terrorist attacks on India's suburban trains. The LeQ is suspected to be a front organization for the Pakistan-based Lashkar-e-Toiba (LeT).[151]

Tactics: Operatives placed suitcases containing the explosives on the luggage racks in the trains. The Maharashtra state government's Anti-Terrorist Squad indicated that a deadly cocktail of RDX, ammonium nitrate, and fuel oil was used in the blasts. They were triggered by a mechanical pencil timer.[152]

e. India-Pakistan, Train Attack – February 18, 2007

Overview: On February 18, 2007, a series of bombs exploded on a train near Diwana, causing a fire that killed at least sixty-six people and injuring fifty others. The train, the Smajhauta Friendship Express, was traveling from Delhi to Pakistan, and carrying over 750 people. This service was recently resumed in January 2004, after being shut down for thirty years because of the conflict between the two countries over Kashmir. The bombs on the train were attached to bottles of kerosene. The attack occurred at midnight, the night before Pakistan's Foreign Minister Khurshid Kasuri was scheduled to visit India. The primary objective of the terrorists was to derail the improved relationship between India and Pakistan.[153]

Terrorist Group: No group has claimed responsibility.

Tactics: Authorities searching undamaged train cars found two suitcases packed with crude, unexploded bombs, and bottles of gasoline, apparently similar to the devices that exploded.[154]

[151] Global Terrorism Analysis, Jamestown Foundation web site http://www.jamestown.org/terrorism/search.php (Accessed on October 31, 2007).

[152] Ibid.

[153] MIPT Terrorism Knowledge Base web site.

[154] Ibid.

3. Terror Threat to Passenger Rail Transportation for New York and New Jersey

While transportation security officials have long been aware of the possible threat of terrorist attacks on transportation networks, these tragic events revealed vulnerabilities in security systems, as well as the consequences of such breaches. Passenger rail transportation systems are, in general, easy and effective targets.

As early as 2002, the FBI issued a warning that Al Qaeda might be planning to attack passenger trains by using operatives who had a Western appearance. The FBI statement had additional information suggesting that operatives might try a variety of attack strategies, such as destroying key rail bridges and sections of track to cause derailments.[155] The FBI warning was not specific to a target location in the U.S. However, past threats have identified that the New York/New Jersey passenger rail systems is on the radar screen for most terrorists. There have been three known terror plots targeting the New York City subway system, all of which were disrupted.

a. Attempted Suicide Bombing Attack – July 31, 1997

On July 31, 1997, New York City police officers successfully averted a nail-filled pipe bomb attack on a Brooklyn subway station that was frequented by Orthodox Jews. The attack was to be carried out by two Palestinian immigrants — Gazi Ibrahim Abu Mezer and Lafi Khalil. Police were tipped off to the attack by Mezer's roommate. In November 1996, Khalil had received a transit visa from the U.S. Consulate in Jerusalem for travel through the United States to Ecuador. But Khalil didn't go to Ecuador. Instead, he boarded a flight to Syracuse, New York, and remained in the U.S. until his arrest in July 1997. Kahlil was convicted of having a fake immigration card; he spent three years in jail and was then deported. Mezer was arrested and sentenced to life in prison.[156]

[155] Joel Brinkley, "F.B.I. Issues a Terror Warning, Citing Possible Threat to Trains," *New York Times*, October 25, 2002.

[156] Detour Ahead Critical Vulnerabilities in America's Rail and Mass Transit Security Programs, Congressional Report prepared by the Democratic Staff of the Committee on Homeland Security, 7.

b. Al Qaeda Hydrogen Cyanide Attack – January, 2003

Ron Suskind, in his book, *The One Percent Doctrine, Deep Inside America's Pursuit of Its Enemies Since 9/11*, reports that, in 2003, al Qaeda had a terror plot well underway targeting the U.S. It was a hydrogen cyanide attack planned for the New York City subways. Al Qaeda cell members had traveled to New York through North Africa in 2002 to identify locations for the attacks. The poison gas would be released through mubtakkars,[157] which would be placed in subway cars and activated remotely. This attack was well past conception and early planning. However, forty-five days before the attacks, Ayman al-Zawahiri, Osama bin-Laden's number two man, called it off.[158]

c. Herald Square Subway Bombing Plot – August 27, 2004

On August 27, 2004, three days before the Republican National Convention, Shahawar Matin Siraj and his co-conspirator James Elshafay were arrested for planning to attack the Herald Square station in New York City with bombs in their backpacks.[159] Prosecutors said the men wanted to avenge the abuse of prisoners at the Abu Ghraib prison in Iraq. At the time of the arrests, the authorities said that the men never obtained explosives and had not been linked to known terrorist groups. James Elshafay pleaded guilty and testified against the mastermind of the plot, Shahawar Matin Siraj, who was sentenced in January 2007 to thirty years in prison.[160]

These terror plots indicate that the NYC subway system is an attractive target to terrorists. The NYC subway system is a component of a much larger network operated by the Metropolitan Transit Authority (MTA). The MTA is the largest in North America, serving a population of 14.6 million people in the 5,000 square-mile area,

[157] A" mubtakkar" (Arabic for inventive) is a gas-dispersal system that can effectively distribute hydrogen-cyanide gas, which is deadly when inhaled.

[158] Ron Suskind, *The One Percent Doctrine: Deep Inside America's Pursuit of its Enemies Since 9/11* (New York, NY: Simon & Schuster, 2006), 218.

[159] Detour *Ahead Critical Vulnerabilities in America's Rail and Mass Transit Security Programs,* 7.

[160] Metro Briefing New York, Manhattan: "Man Gets Five Years In Plot To Bomb Subway,*" New York Times,* March 3, 2007.

fanning out from New York City through Long Island, southeastern New York state, and Connecticut. The NYC subway system alone covers the Boroughs of Manhattan: Bronx, Brooklyn, Queens, and Staten Island. There are 468 subway stations, twenty-six subway lines, and 6,241 subway cars.[161] Given its composition, the NYC subway system is very open and accessible, with fixed, predictable access points. The system's openness would make it easy for potential terrorists to hide in crowds without arousing suspicion. Securing such a system presents transit officials and the New York City Police Department (NYPD) with daunting challenges.

Just across the Hudson River, in New Jersey, is another highly accessible passenger rail network. NJ TRANSIT covers a service area of 5,325 square miles and is the nation's third largest provider of bus, rail, and light rail transit, linking major points in New Jersey, New York, and Philadelphia. The passenger rail system is comprised of eleven trains and forty-five light-rail vehicles. NJ TRANSIT provides nearly 223 million passenger trips each year.[162] It is interconnected with the Port Authority Trans-Hudson (PATH) system at various stations. PATH is a subsidiary of the Port Authority of New York and New Jersey. This heavy rail transit system serves as the primary link between Manhattan and neighboring New Jersey's urban communities and suburban railroads. PATH presently carries 227,000 passengers each weekday.

The PATH transit systems possess a different set of security challenges due to its unique operating structure, and the fact that it runs through tunnels under the Hudson River. *The New York Times* reported that in July 2006, several people were arrested overseas in what authorities said was a plot to bomb the PATH system. The arrests halted what officials said was a bid to set off backpack bombs in a PATH train car, and flood the tunnels. Some published reports said maps and other material relating to the PATH tunnels had been found on the computer of one of those arrested.[163] This threat spiraled into another issue that surfaced regarding the vulnerability of the PATH

[161] Metropolitan Transit Authority web site http://www.mta.info/ (Accessed on November 6, 2007).

[162] New Jersey Transit web site http://www.njtransit.com/tm/tm (Accessed on November 6, 2007).

[163] William K. Rashbaum and William Newman, "PATH Tunnels Seen as Fragile in Bomb Attack," *New York Times*, December 22, 2006.

system. In December 2006, a government official gave a draft summary of an analysis of the PATH system to the *New York Times*. The official said the latest analysis indicated that it would take only six minutes for one of the PATH tubes to flood if a significant, but not necessarily very large, bomb were detonated. The *New York Times* also reported that the analysis appeared to be the most detailed and sophisticated government review of the train tubes' vulnerability. The analysis revealed that the Hudson River tubes, which suffered serious damage in the 2001 terror attack, are more vulnerable than most other tunnels that pass under the city's waterways because they lie in the soft riverbed, unlike other tunnels that are bored through the underlying bedrock. Over the years, silt has built up atop the tubes, which were laid roughly ninety years ago.[164]

4. Analysis and Key Judgments of the New York/New Jersey Passenger Rail System Threat

The foreign incidents represent some of the most recent and high-profile attacks over a four-year period. These attacks, coupled with the threats made against the NYC Subway and PATH systems, illustrate the threat, target, and attack commonalities and characteristics. Based on these commonalities and characteristics, we can develop a threat analysis of the NYC Subway System, NJ TRANSIT, and PATH lines. In addition, the threat analysis will enable us to create a hypothetical attack scenario that targets these systems. Ultimately, the threat analysis is meant to evaluate the effectiveness of the integrative risk management/governance framework and the utility it has for the decision maker when faced with such a critical situation.

A report released by the Department of Justice (DOJ) identifies an essential list of categories that are intended to create a foundation of data prior to conducting a thorough threat assessment. These categories will be the tool used for the threat analysis as it pertains to the New York and New Jersey passenger rail systems.[165]

1. Type/Category of Adversary: Terrorists acting alone or within groups or cells, who are extremely radicalized and willing to take the lives of others, who intend to cause

[164] Rashbaum and Newman, "PATH Tunnels Seen as Fragile in Bomb Attack."

[165] U.S. Department of Justice, "Assessing and Managing the Terrorism Threat," September 2005, 5.

mass destruction, and in some cases take their own lives in order to inflict the greatest amount of harm. They can be categorized as foreign or domestic, terrorist or criminal.[166]

The four young men responsible for the London bombings are a good example of homegrown terrorism. These men (aged 18, 19, 22, and 30) were British citizens. Without prior experience or specific knowledge, they were able to organize four almost simultaneous bombings using homemade organic peroxide devices carried in backpacks. The construction of these devices did not require much expertise; the materials and equipment were readily available, and the plotters financed themselves at the modest cost of around $14,000. The bombs were built in the living room of an ordinary apartment in the city of Leeds. They were detonated manually in suicide attacks. The bombers were in contact with other Islamic extremists in the United Kingdom, but not in a sustained way.[167]

None of the four men had been identified as potential terrorist threats before the July bombings. They were largely invisible to the security services. The bombings showed that it may not be possible to identify significant actors in advance; nothing appeared to distinguish the bombers from other extremists who had not yet moved from talk to action. The radicalization process was apparently very quick, though, progressing rapidly from discussion to execution. The process was one of "self-radicalization." It was not initiated or guided by an Islamic leader or the clerical authority of a radical Imam.[168]

It would be ignorant on our part to think that young Muslim men in the U.S. are not influenced by the global jihadist movement. With advancements in communication and technology, radicalizing potential jihadists through the Internet is not such a far reach. Benjamin and Simon report that what transforms jihadist violence is the ability to disseminate tactics, technical know-how, and strategy. The availability of training materials on the Internet, and targeting guidance that is independent of any vetting

[166] U.S. Department of Justice, "Assessing and Managing the Terrorism Threat," 6.

[167] MIPT, Terrorism: "What's Coming the Mutating Threat," 20.

[168] Ibid., 25.

process, allows volunteers to contribute to the cause immediately. The requirement for joining up is reduced to a simple process of self-selection.[169]

Type/Category of Adversary — Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *Three men ages 19, 20, and 22, all of whom are United States citizens residing in Paterson, N.J., have adopted the principles associated with Islamic radicalism. They are not openly engaged in the fundamental practices of Islamist activism, but confide in one another about their beliefs, ideological direction, and the forward progression of the jihadist movement. With the Presidential Election approaching, Osama bin Laden once again declares war on the U.S. Like all his previous statements, bin Laden's message is unmistakably religious in tone and content. The three Paterson men take Bin Laden's message very seriously, and begin to develop an attack strategy targeting the PATH transit lines.*

2. Objective of Adversary: Theft, sabotage, mass destruction, inflicting harm on innocent individuals that results in multiple casualties, impacting economic vitality, and ultimately make a socio-political statement. [170]

Some of the global attacks to passenger rail indicate that the core objective of the adversary was to maximize casualties and affect the socio-political positions within the country. The Madrid and London bombers were extremely radicalized. The religiously driven terrorists of the current era are distinguished from their more secular predecessors in their desire to kill large numbers of people on an indiscriminate basis; the 9/11 attacks and later operations carried out by Al Qaeda-linked groups in Bali and Casablanca and other locales illustrate this.[171]

In addition to mass casualties, the Madrid and India-Pakistan attacks also had socio-political implications linked to their objectives — to affect the election of the Prime Minister in Spain, and to derail the improved relationship between India and Pakistan. On the domestic front, Shahawar Matin Siraj and James Elshafay were arrested for plotting to bomb the Herald Square station in New York City. Their objective was to avenge the abuse of prisoners at the Abu Ghraib prison in Iraq, yet another socio-political statement.

[169] Benjamin and Simon, *The Next Attack, 75*.

[170] U.S. Department of Justice, "Assessing and Managing the Terrorism Threat," September 2005, 6.

[171] MIPT Terrorism: "What's Coming the Mutating Threat," 43.

In either case, whether the objectives were driven by religion or socio-political statements, there was a distinct association with the radical Islamist movement. Hoffman states that the "…religious motive is overriding and indeed, the religious imperative for terrorism is the most important defining characteristic of terrorist activity today."[172]

Objective of Adversary — Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *The Paterson group has adopted the principles associated with Islamic radicalism. They are individuals driven by a religious ideology. Therefore, violence is first and foremost a sacramental act or a divine duty executed in direct response to some theological demand or imperative. In this case it is bin Laden's message.*[173] *The objective is to kill as many passengers as possible on the PATH transit line from New Jersey to New York, in response to bin Laden's message.*

3. Number of Adversaries: Operatives acting within a coordinated cell or group of terrorists. The individual suicide bomber acting alone with no outside or group support.[174]

The individuals who executed the attacks in Madrid, London, and Mumbai were for the most part not intricately involved with an interconnected terrorist organization. In each case, however, the important point was that the groups were essentially local, but were inspired or emboldened by a global cause. The National Intelligence Estimate depicts this global jihadist movement, which includes the remnants of Al Qaeda as well as local affiliates and imitators, as one that is spreading around the world. Self-radicalization at the individual level and self-generated cells at the organizational level are becoming more common.[175]

[172] Hoffman, *Inside Terrorism: Revised and Expanded Edition* (New York: Columbia University Press, 2006), 82.

[173] Ibid., 88.

[174] U.S. Department of Justice, "Assessing and Managing the Terrorism Threat," September 2005, 6.

[175] MIPT Terrorism: "What's Coming the Mutating Threat," 19.

Number of Adversaries — Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *The Paterson group is not linked to any external terrorist organization or cell. They do not need particular skills or resources in order to cause massive loss of life. They are self-radicalized and share knowledge retrieved from the Internet regarding tactics and target execution. The clerical authority that will legitimize their actions is solely in the words of bin Laden.*

4. Target Selected by Adversary: Critical infrastructure, government buildings, national monuments.[176]

The transnational historical perspective of the passenger rail threat was conducted to examine the possibility of passenger rail being targeted in the New York/New Jersey region. It was evident that this component of critical infrastructure would be difficult to protect and defend against any attack. It is an exceedingly soft target, and will continue to be an attractive one to terrorists.

Target Selected by Adversary — Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *On several occasions the three members of the Paterson Group have traveled the PATH train from Exchange Place in Jersey City to the World Trade Center stop in lower Manhattan. They have agreed that due to the high volume of passengers on the PATH during rush hours, and the criticality that this mass transit system has to both venues, it would make for a prime target, and answer the calling of bin Laden's message.*

5. Type of Planning Activities Required Accomplishing the Objective: Casing and photographing high-volume passenger rail systems and locations in the region. Maps and scheduling information are available on the web. Observation of security, easy access points, and high-volume travel lines. The openness of the system makes it difficult to detect reconnaissance operations conducted by an adversary. The London bombers were observed on-camera while executing the attack. There was no behavioral indication that would have alerted authorities to take action in order to prevent the attack. The same can be said for other individuals who may be observing the passenger rail environment with expectation of carrying out an attack.

[176] U.S. Department of Justice, "Assessing and Managing the Terrorism Threat," September 2005, 6.

Type of Planning Activities Required Accomplishing the Objective - Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *The Paterson group has utilized the high volume of pedestrian traffic as concealment during reconnaissance operations of the PATH lines. They have timed departure and arrival times in order to identify when the train would be in the tube under the Hudson River. No photos were necessary; maps and schedules were retrieved from the Internet.*

6. Most Likely "Worst Case" Time an Adversary Could Attack: Past attacks indicate that rush hour is the optimal time. Passenger density and volume is at its peak, which will increase the number of casualties. Platforms at major rail exchanges are also a primary concern due to the high volume of transients. Previous attacks illustrate such a pattern:

- Moscow, Russia, metro bombing – 8:40 a.m., morning rush hour
- Madrid, Spain, train bombings – 7:45a.m., morning rush hour
- London, England, transit bombings – 8:50 a.m. and 9:47 a.m., morning rush hour
- Mumbai, India, train attacks – 6:30 p.m., evening rush hour[177]

Most Likely "Worst Case" Time an Adversary Could Attack - Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *Through observation and surveillance, the Exchange Place stop is at peak volume between 8:10 a.m. and 8:45 a.m. The Paterson group has identified this time-window as the optimal time for execution.*

7. Range of Adversary Tactics: The tactics utilized have primarily focused on remote detonation with timing devices, as was the case of the Madrid, Mumbai, and India-Pakistan attacks. Bags and backpacks were obscured from passenger view in racks and under seats.

One of the most lethal tactics is that of the suicide bomber. Terrorists have become increasingly attracted to suicide attacks because of their unique tactical advantages, compared to those of more conventional terrorist operations. Suicide tactics

[177] MIPT Terrorism Knowledge Base web.

are devastatingly effective, lethally efficient, have a greater likelihood of success, and are relatively inexpensive.[178] Past passenger rail attacks indicate that attacks underground or in tunnels have significant consequences, as with the London and Mumbai bombings. In addition, self detonation is less complex than remote timing devices. This can be appealing to the homegrown terrorist, who is less sophisticated than an operational terrorist group.

Fathali M. Moghaddam, in his book *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy*, points out that what makes suicide terrorism strategically effective is that it is very difficult, in practice perhaps impossible, to guard against. Modern economies rely on mass movements of people, particularly in and around major urban centers that house millions of people from different ethnic, religious, and national backgrounds. The diversity of the people who move across borders and in and out of major urban centers makes it even more difficult to screen for suicide terrorists. The July 2005 suicide bombings in London illustrate this point: These four homegrown suicide bombers were part of immigrant communities that settled in England but had ties to radicals in Pakistan. In essence, these were "terrorists without borders," who executed a plan to bring the London transportation system to a standstill.[179]

Range of Adversary Tactics — Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *In his book Dying to Win: The Strategic Logic of Suicide Terrorism, Robert Pape points out a significant component, which is common with the Paterson Group, is that suicide bombers often work in teams. In fact, many suicide attacks involve multiple individuals working together for long periods of time to gather intelligence, plan, and rehearse the mission. Team suicide attacks, by their nature, are based on extensive social interaction and require unity of purpose, features that are more likely associated with altruistic motives.[180] The Patterson group is committed to making the ultimate self-sacrifice by targeting the PATH system utilizing themselves as the destructive device. Their radicalism and call to honor bin Laden is their motivation.*

[178] Hoffman, *Inside Terrorism: Revised and Expanded Edition*, 132.

[179] Fathali M. Moghaddam, *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy* (Westport, Connecticut: Praeger Security International, 2006), 123-124.

[180] Robert A. Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005), 185.

8. Capabilities of Adversary: Past incidents reveal that most attacks are carefully planned and executed. Knowledge and skillful adversaries can easily weaponize devices that contain gasoline components and create incendiary effects. More skillful adversaries, who can obtain resources to build explosive devices, pose a greater threat. The London bombers utilized homemade organic peroxide devices carried in backpacks.[181] Although these were highly unstable, the expertise to make these devices did not take great skill.

Range of Adversary Tactics - Hypothetical Scenario Targeting the Passenger Rail System of New York/New Jersey: *The Paterson group is made up of educated young men. Although they have no formal training with explosives, the eldest of the three attends New York University and is pursuing a degree in biology. Chemistry is a requirement for the curriculum, and has provided him with a basic understanding of combining chemical compounds. He is advanced enough to create a device comprised of hexamethylene triperoxide (TATP), the explosive used by the London bombers. His objective is to create three devices, all of which are designed to be self-detonating.*

The threat analysis for the NY/NJ Passenger Rail System, coupled with the hypothetical scenario of the Paterson Group, is designed to create a foundation for conducting an evaluation of the risk management/governance framework. The homeland security problem space is too large for a risk management framework that is intended to cut across multiple problem areas. By narrowing down the scope to a sector/region-specific threat, the elements of the risk management/governance framework can be adequately evaluated. The hypothetical scenario was developed to assist with the logical findings of the risk management/governance framework as an application for homeland security decision makers. The threat analysis covers eight categories essential for collecting data, which can be further filtered through a thorough threat assessment process. Each category correlated with the hypothetical scenario, painting a picture of a possible terrorist attack against the PATH Passenger Rail Lines.

[181] MIPT Terrorism: “What’s Coming the Mutating Threat,” 20.

B. RISK PERCEPTION AND THE PASSENGER RAIL THREAT

1. Risk Perception and the Risk Management Framework Correlation

The public's reaction to the events of September 11 and its aftermath provide an important insight into the psychology of risk perception and response to risk. For example, it demonstrates the selective nature of focusing attention on different sources of risk or danger. Paul Slovic points out that, through the process of risk amplification, the adverse impact of such an event sometimes extends far beyond the direct damage to victims and property, and may result in massive indirect effects.[182] The indirect effect of September 11 made Americans realize they are no longer safe, and are vulnerable to international terrorist attacks inside U.S. borders. This has changed America's perception of terrorism risk.

Risk perception is the subjective assessment of the probability of a specified type of accident happening, in this case a threat or attack to passenger rail, and how concerned one is with the consequences. To perceive risk requires an evaluation of the probability as well as the consequence of a negative outcome. Perception of risk goes beyond the individual. It is a social and cultural construct reflecting values, symbols, history, and ideology.[183] Policy makers need a better understanding of how the public perceives risk in general and the specific risks associated with terrorism. Risk management decisions may be influenced by public perceptions of risk, which may result in a shift of resource allocations or operational deployment strategies.

The risk management/governance framework analyzed for this study provides a logical set of actions that can produce an effective methodology for decision makers to follow. By further researching the components of public risk perception and the passenger rail threat, we can identify whether the risk management/governance framework takes public perception into account.

[182] Paul Slovic and Elke Weber, "Perception of Risk Posed by Extreme Events," Paper presented at the conference Risk Management Strategies in an Uncertain World, Palisades, New York, April 12-13, 2002, 12.

[183] Lennart Sjoberg, Bjorg-Elin Moen, Torbjorn Rundmo, *Explaining Risk Perception: An Evaluation of the Psychometric Paradigm in Risk Perception Research*, Trondheim, Norway: Norwegian University of Science and Technology, 2004, 8.

2. Risk Perception and Terrorism

Suppose for a moment that the Port Authority of New York/New Jersey receives a threat that large vehicle truck bombs containing radioactive material will be detonated in the tubes of both the Lincoln and Holland Tunnels. Both tunnels are shut down immediately, and all other Hudson River crossings are placed on high alert. Traffic diversion plans are implemented on both sides of the river, resulting in a transportation nightmare. Within thirty-six hours, DHS announces that the threat has passed. However, the Port Authority continues to divert trucks to other Hudson River crossings, causing immense traffic jams and motorist confusion. People begin to leave their vehicles at home due to the increased delays, and start to use the PATH train to travel into Manhattan. The PATH system is now packed with people, making it a most undesirable means of transportation. This illustration demonstrates the importance of perceived risk regarding terrorism: The perception of risk — regardless of whether a threat is actually present — is sufficient to cause widespread disruption. Understanding how specific factors drive the perception of risk is essential to understanding how people will respond to threats of terrorism.[184]

Since there have been a limited number of terror-related attacks on U.S. soil, it is unclear how Americans perceive the likelihood of an attack, to the consequences of different types of attacks and how the public might respond. Understanding the terrorist threat is critical to maintaining public morale, sustaining economic activity, and limiting disruption to normal daily routines. Obtaining a deeper understanding of how Americans perceive the terrorist threat will assist the development of policies and procedures for educating and preparing the nation for the impact of an act of terrorism, if it were to occur.[185]

Paul Slovic, in his book *The Perception of Risk*, discusses the utility of the psychometric paradigm to measure the public's perception of risk. The psychometric

[184] Clinton M. Jenkin, "Risk Perception and Terrorism: Applying the Psychometric Paradigm," *Homeland Security Affairs* II, no. 2 (July 2006), 1.

[185] The Society for Risk Analysis, http://www.sra.org/events_2007_meeting.php [Accessed December 18, 2007].

paradigm is a theoretical framework that assumes risk is subjectively defined by individuals who may be influenced by a wide array of psychological, social, institutional and cultural factors. The paradigm assumes that, with appropriate design of survey instruments, many of these factors and their interrelationships can be quantified and modeled in order to illuminate the response of individuals and their societies to the hazards that confront them.[186] Slovic refers to this psychometric paradigm as a strategy for studying perceived risk by developing classifications of hazards that can be used to understand and predict responses. Within the paradigm, people make quantitative judgments about the current and desired riskiness of diverse hazards, and the desired level of regulation of each.[187]

In Clinton Jenkin's article, "Risk Perception: Applying the Psychometric Paradigm," he explains that psychometric studies have examined numerous dimensions of risk for scores of hazards. The commonly used dimensions are listed in Table 2.[188]

[186] Paul Slovic, *The Perception of Risk* (London: Earthscan Publications Ltd, 2000), xxiii.

[187] Ibid., 222.

[188] Jenkin, "Risk Perception and Terrorism,"7.

Table 2. Qualitative Dimensions of Risk Used in the Psychometric Paradigm[189]

Voluntariness	The extent to which exposure to the hazard is voluntary.
Immediacy	The extent to which the consequences are noticed immediately.
Knowledge of exposure	The extent to which a person knows if he/she has been exposed.
Expert knowledge	The extent to which experts know about the hazard.
*Controllability**	The extent to which a victim can control the severity of consequences due to exposure.
Novelty	The extent to which the hazard is new to society.
*Catastrophic potential**	How many fatalities occur at once.
*Dread**	The extent to which the effects of exposure are dreaded.
*Severity**	The extent to which the consequences of exposure are severe.
Delayed	The extent to which the consequences of exposure are delayed.
*Certainly fatal**	The extent to which exposure will definitely cause fatality.
*Increasing**	The extent to which the risk is increasing over time.
*Preventability**	The extent to which the hazard is preventable.
*Inequitable**	The extent to which risks and benefits are not equally distributed across society.
*Affects future generations**	The extent to which the hazard will affect future generations.
*Global catastrophe**	The extent to which the hazard threatens a global catastrophe.
*Easily reduced**	The extent to which risk associated with the hazard can be easily reduced.
*Personal impact**	The extent to which the risk affects the respondent personally.
Observability	The extent to which the effects of exposure are observable.

Dimensions marked with a (*) were directly correlated with perceptions of risk[190]

[189] Jenkin, “Risk Perception and Terrorism,” 8.

[190] Ibid.

This multitude of dimensions can lead to very cumbersome research designs, so most risk studies include the dimensions most applicable to the study at hand. For example, a terrorism study may elect to exclude inequatability because the inequity of terrorism risk is not likely to be an issue, as it might be for the risk of a toxic waste dump or nuclear power plant.[191]

For the purposes of this research and correlation to the risk management frameworks, we can look at the dimensions of risk using the Psychometric Paradigm, and draw from it a matrix that is specific to the threat associated with passenger rail transportation. The matrix in Table 3 will provide us with a public risk perception (PRP) outlook that can be drawn upon during the risk management/governance framework evaluation.

[191] Jenkin, "Risk Perception and Terrorism," 7.

Table 3. Qualitative Dimensions for Public Risk Perception Matrix as it Pertains to Passenger Rail Transportation

Expert knowledge	The extent to which experts know about the hazard. **PRP:** The public's reliance on the intelligence community's ability to collect data indicating a threat directed at passenger rail transportation.
*Controllability**	The extent to which a victim can control the severity of consequences due to exposure. **PRP:** Consequences can be mitigated due to a timely first responder element.
Novelty	The extent to which the hazard is new to society. **PRP:** Terrorism targeting passenger rail is prominent on a global stage, and has had domestic implications in the U.S.
*Catastrophic potential**	How many fatalities occur at once. **PRP:** Potential consequences of fatalities is determined by method of attack and targeted location.
*Severity**	The extent to which the consequences of exposure are severe. **PRP:** Severity of the attack is determined by method of attack, target location, cascading affects, public fear.
*Increasing**	The extent to which the risk is increasing over time. **PRP:** Transnational attacks and domestic threats to passenger rail will increase the risk.
*Preventability**	The extent to which the hazard is preventable. **PRP:** The openness of passenger rail transportation makes it difficult to prevent an attack from being executed.
*Easily reduced**	The extent to which risk associated with the hazard can be easily reduced. **PRP:** Protection measures can be implemented, however, the risk is not easily reduced due to the vulnerabilities associated with passenger rail.

Models that gauge risk perception and that can be applied to terrorism are difficult to evaluate. In the book *Psychology of Terrorism*, the authors suggest that two factors may be central to understanding how people assign values to terrorist incidents. The first factor can be described as "dread risk," a continuum beginning with low-dread events, which are seen as controllable, not catastrophic, decreasing in risk over time, and generating little risk for future generations. Conversely, high-dread events are viewed as having a high mortality rate, being globally catastrophic and inescapable, and increasing in risk over time.[192][193]

[192] Bruce Bongar et al., *Psychology of Terrorism*, Oxford, New York: Oxford University Press, 2007, 35.

[193] Slovic and Weber, "Perceptions of Risk Posed by Extreme Events," 10.

A second factor is “unknown risk,” which begins at the low-risk level with well-understood, observable, non-novel events. If an event is high on the unknown risk dimension, it is characterized by having a delayed or persisting effect, and being a novel threat that is poorly understood.[194]

In evaluating the “dread risk” factor, the public perception of a terrorist attack being carried out against passenger rail will be considered low. However, add to the equation a transnational terrorist attack that targets the London underground, killing hundreds of people, followed by a credible threat against passenger rail for the NYC subway system, and the “dread risk” factor becomes a “high dread” event. The “unknown risk” factor for an attack targeting passenger rail is, for the most part, considered a low-risk level in the absence of a credible threat.

To illustrate the “dread risk” and “unknown risk” factors, we can look at the October 6, 2005, threat against the NYC subway system. FBI and DHS intelligence sources indicated that nineteen operatives had been deployed to New York to target the system. Although the intelligence turned out to be non-credible, NYC Police Commissioner Ray Kelly and NYC Mayor Michael Bloomberg immediately implemented protective security measures by increasing police patrols, explosive detection canines, and random bag and package searches.[195] Without threat intelligence, the “dread risk” and “unknown risk” factors remained low. The heightened security and elevated alert status associated with this threat, however, increased both the “dread risk” and “unknown risk” factor.

[194] Bongar et al., *Psychology of Terrorism*, 35.

[195] ABC News website, “Police Investigate New York Subway Terror Threat,” October 6, 2005 http://abcnews.go.com/US/story?id=1190231 [Accessed on December 27, 2007].

THIS PAGE INTENTIONALLY LEFT BLANK

V. AN INTEGRATIVE RISK MANAGEMENT/GOVERNANCE FRAMEWORK FOR HOMELAND SECURITY DECISION MAKING

A. INTELLIGENCE SIMULATION FOR TERROR THREAT TO THE PASSENGER RAIL SYSTEM

1. Introduction

Chapter IV provided a qualitative risk and threat analysis based on three underlying threat analysis factors that are central to the passenger rail transportation sector: global attacks and threats to passenger rail transit systems; the terror threat to passenger rail transportation for New York and New Jersey; and analysis and key judgments of the New York/New Jersey passenger rail system. Based on this analysis, a hypothetical scenario was matched with categories that are intended to create a foundation of data prior to conducting a thorough threat assessment. This segment of the chapter is meant to simulate intelligence that has been collected, processed, and disseminated based on the hypothetical scenario.

2. Intelligence Threat Simulation

The Integrative Risk Management/Governance Framework can be applied to a variety of homeland security issues in order to evaluate the process. Rather than focus on resource allocation and cost-effective strategies, threat intelligence and strategic operational deployment strategies will be the primary driver for the framework. Earlier in this paper, we examined wicked problems and how they could be applied to the passenger rail transportation threat environment:

- Screen every passenger or conduct random screening?
- Screen every passenger and cause extensive delays in commuter operations?
- Identify a threat when there is a great deal of intelligence, but nothing specific.
- Identify a threat when there is no credible intelligence targeting passenger rail.
- Identify the appropriate response when there is tactical intelligence of a threat targeting passenger rail, and that intelligence is specific to cell operations.

Clearly these are a set of issues that would intensify based on data that is collected, processed, and vetted through the intelligence cycle. A daunting challenge of the intelligence community evolves around what is relevant and what is actionable. How do we extract the desired intelligence from a mountain of information, and use it to drive down risk?

Threat Intelligence Simulation for Passenger Rail System of New York/New Jersey

With the 2008 Presidential election approaching, Osama bin Laden once again declares war on the U.S. Like all his previous statements, bin Laden's message is unmistakably religious in tone and content. The underlying factor that emerges is, "Attack U.S. citizens on American soil." The three Paterson men take Bin Laden's message very seriously, and begin to develop an attack strategy targeting the PATH transit lines.

Bin Laden's message has caused a recent increase in intelligence "chatter," which might indicate an imminent terrorist attack. The U.S. intelligence community has begun to monitor this chatter; they examine not the content of communications intercepts, but the volume. Analysts and intelligence operatives are paying close attention to fluctuations in the number of messages sent and received over networks used by known and suspected terrorists.

Until now, the Paterson group has been operating on its own, without any transnational influence. They are purely homegrown radicalized individuals, but feel the desire to make contact with al Qaeda operatives in the Middle East, and inform them of their plans. One of the Paterson men has made contact with an individual on the national watch list. Throwaway cell phones, computer kiosks located in New York and New Jersey, and various Internet cafes have enabled the men to use a different network each time they communicate with this transnational operative.

Intelligence agencies have noticed volume spikes on several networks, and have compared them with the content of recent local (NY/NJ) communications intercepts, satellite observations abroad, and information passed to intelligence operatives in other countries.

Although there is no intelligence on the capability of an adversary, a pattern has emerged that indicates the possibility of an explosive attack on the passenger rail systems of New York and New Jersey.

B. APPLIED INTEGRATIVE RISK MANAGEMENT/GOVERNANCE FRAMEWORK TO TERROR THREAT FOR PASSENGER RAIL TRANSPORTATION SYSTEM

1. Introduction

The intelligence threat simulation has been constructed to necessitate courses of action taken by federal, state, and local leaders that are responsible for managing risk in the New York/New Jersey region. The Integrative Risk Management/Governance Framework will provide the process that a homeland security decision maker may choose to use as a guide when making decisions how to respond to the threat. The methodology utilized for the framework analysis in Chapter III will be consistent with this framework, with the exception of integrating the analytical, intuitive, and capability-based decision making with the strategic, operational, and tactical decision-making processes. Examples will be provided to illustrate the various processes, networks, entity capabilities, and risk assessment methodologies that support the decision maker. They are by no means exhaustive; they are supporting elements.

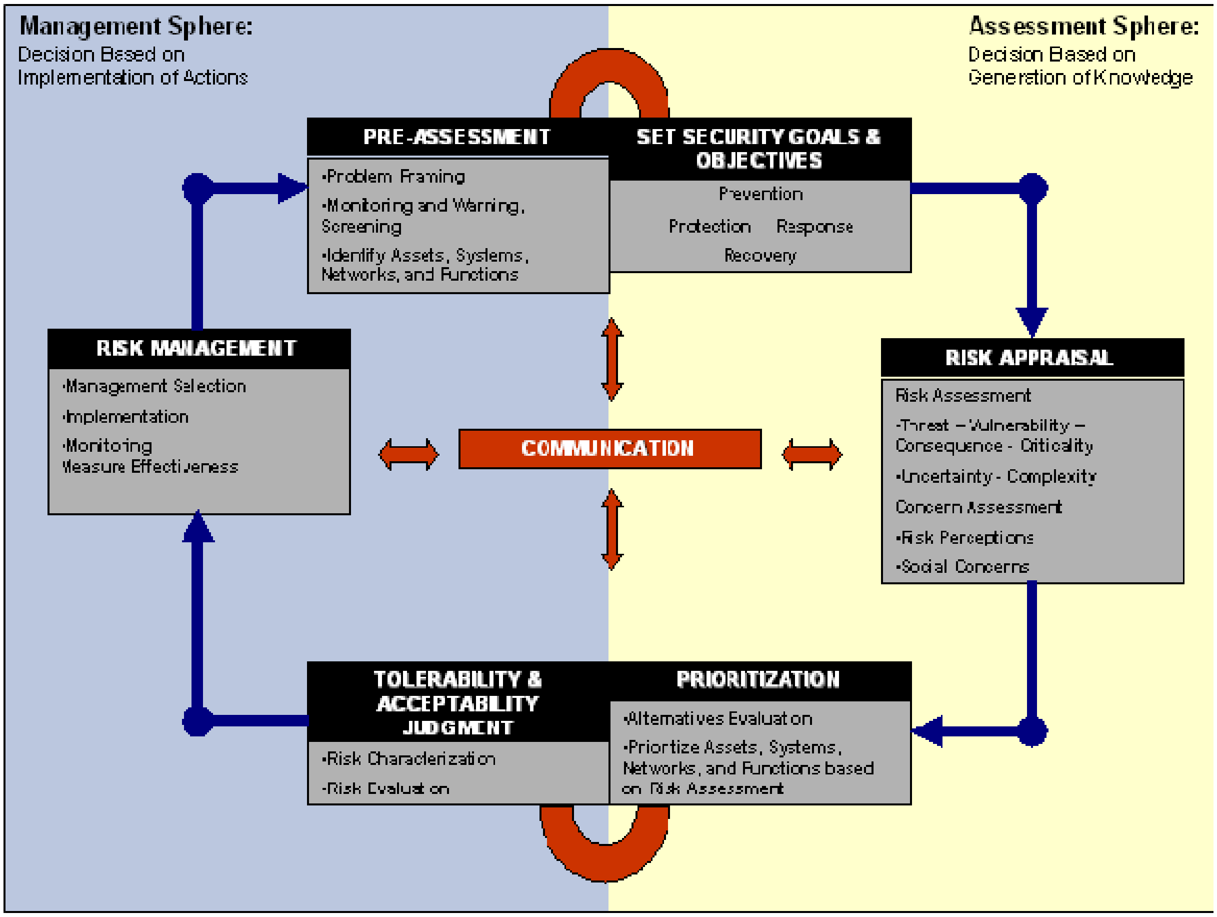
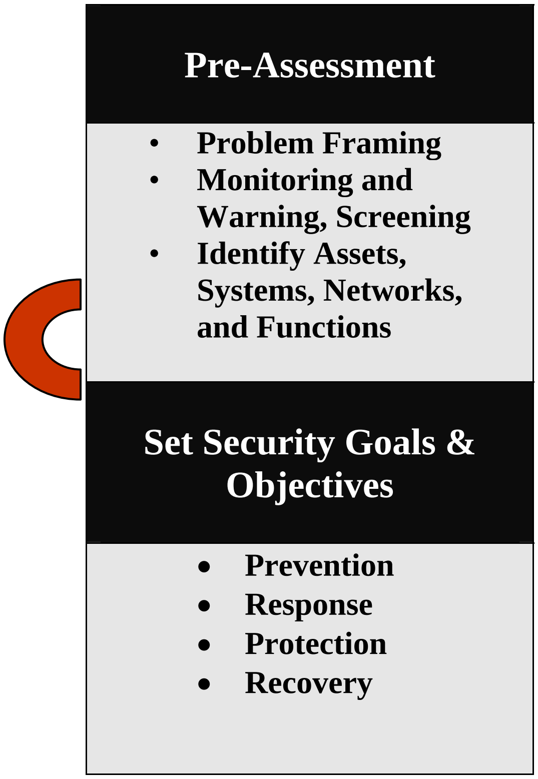


Figure 12. Integrative Risk Management/Governance Framework

2. Final Analysis, Implementation and Evaluation of Applied Framework



Pre-Assessment

- **Problem Framing**
- **Monitoring and Warning, Screening**
- **Identify Assets, Systems, Networks, and Functions**

Set Security Goals & Objectives

- **Prevention**
- **Response**
- **Protection**
- **Recovery**

The Pre-Assessment and Set Security Goals and Objectives Components provide a starting point for the decision maker in developing a strategy that can be applied to best manage risk, and prevent an attack from occurring on the passenger rail systems of NY/NJ. Each of these components provide the decision maker with elements that can guide decisions, whether they are based on the implementation actions that are relevant to the Management Sphere, or the generation of knowledge, which is relevant to the Assessment Sphere. Collectively, both components provide a foundation and building block that will guide the decision-making process, and support a seamless transition into the Risk Appraisal phase.

Pre-Assessment / Set Security Goals & Objectives	
Strategic DM	The Strategic DM can utilize these components to develop a course of action to best prevent an attack from being carried out against the passenger rail system of NY/NJ. Problem framing will assist with developing goals and objectives for each of the mission areas (prevention, protection, response, recovery). An intricate element for problem framing will be the collection, processing, and dissemination of actionable intelligence. All relevant intelligence agencies can utilize the problem framing principle to categorize the significance of the threat. Monitoring and warning, and screening tools are identified and will support each of the mission areas by providing real-time situational awareness and monitoring of the operational environment. This component enables the Strategic DM to develop goals and objectives so that Operational and Tactical decision makers can carry out the Strategic DM intent and course of action.
Examples:	**Problem Framing:** Agencies that support this element include FBI Joint Terrorism Task Force (JTTF), DHS, TSA, NYPD, Port Authority Police Department (PAPD), New Jersey State Police (NJSP), NJ Transit, and the Port Authority of NY/NJ. **Monitoring & Warning: I**nformation sharing takes place among the Homeland Security Information Network (HSIN), NYPD Command and Control Center, NYPD Regional Intelligence Center (RIC), NJ Regional Operations Intelligence Center (ROIC), NY/NJ Regional Information Sharing Environment (RISE).
Operational DM	The Operational DM can develop operationally based strategies to support the mission areas. First and foremost will be prevention. The Operational DM can utilize problem framing to determine what passenger rail transportation nodes are most critical, and can utilize monitoring and warning, and screening to identify the areas with the highest passenger volume, and then determine the operational objectives to best protect and defend those areas. In addition, close coordination with intelligence factions helps to prevent impeding on immediate action measures. The Operational DM can identify capabilities and analytical products to support deployment goals.
Examples:	**Problem Framing:** To support mission areas. **Prevention:** Layered security approach throughout rail transportation system conducted by NYPD, PAPD, NJ Transit, NJSP. The goals and objectives for this approach should be oriented toward achieving optimal enforcement in order to deter, disrupt, or mitigate the impact of a terrorist attack, which could include physical modifications, technologies, and passenger bag screening. **Monitoring & Warning:** Information sharing takes place among analytical fusion centers and NYPD-RIC, NJ-ROIC, and NY/NJ-RISE.
Tactical DM	The Tactical DM can support operational goals and objectives by identifying the necessary tactical elements needed to best support the mission areas. The Tactical DM can utilize problem framing, monitoring and warning to identify the specificity of the threat. If intelligence indicates that explosives are the primary method of attack, the Tactical DM can support the strategic goals and objectives by identifying deterrence strategies. The Tactical DM may call upon Intuitive DM if an attack is imminent.
Examples:	**Problem Framing, Monitoring & Warning:** Explosive attack modus operandi – regional law enforcement entities can deploy explosive detection K9 teams, NYPD explosive trace detection elements, container bag screening.

Risk Appraisal

Risk Assessment

- **Threat – Vulnerability – Consequence - Criticality**
- **Uncertainty - Complexity**

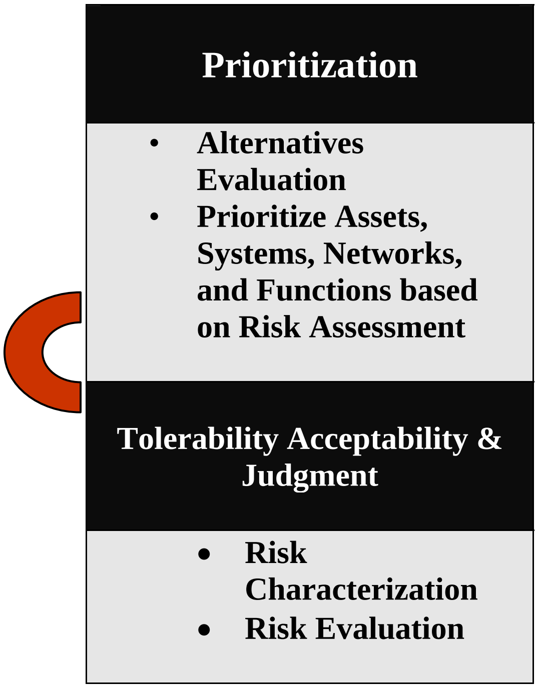
Concern Assessment

- **Risk Perceptions**
- **Social Concerns**

The Risk Appraisal Component is a combination of risk assessment and concern assessment. The risk assessment contains the essential elements of threat, vulnerability, consequence, and criticality. Uncertainty and complexity are elements as well, and reflect the difficult challenges decision makers have when threat of attack is uncertain, and the complexity of the infrastructure, such as the rail transportation system, is so vast and open. Concern assessment contains the elements of risk perception and social concern. The Qualitative Dimensions for Public Risk Perception Matrix as it pertains to Passenger Rail Transportation (Table 3 in Chapter IV) examined the fear and dread associated with a terrorist attack directed at the passenger rail system. It illustrated that risk management decisions can be influenced by the public perception of risk, which may result in a shift of operational deployment strategies. Based on the threat simulation, decision makers must consider all elements that are central to the risk assessment, and factor in the risk perceptions and social concerns as well.

Risk Appraisal	
Strategic DM	The Strategic DM can utilize the Risk Appraisal Component by first looking at the risk assessment. The elements of threat, vulnerability, consequence, and criticality can assist the Strategic DM through an analytical approach in order to identify a proven risk assessment methodology that is appropriately tailored for an explosive attack to passenger rail transportation. Uncertainty and complexity is high during the Strategic DM process due to the nature of the threat. The Strategic DM must take into account risk perception and social concerns as well. The public must be informed through public awareness strategies, which may also act as deterrence measures.
Examples:	**Threat Analysis:** Generated actionable intelligence products that can support the Strategic DM through collaborative efforts. Facilitated by the FBI-JIC, NYPD-RIC, NJSP-ROIC. **Vulnerability Assessments (VA):** Current documentation identifying vulnerabilities to the rail transportation sector for NY/NJ. The VA should be specific to the intent and capability of the adversary. Tools should be tailored to the threat in question.

	Consequence Analysis (CA): Identifying the highest level of risk based on loss of life and the cascading impact to other infrastructure. This includes quantitative consequence analysis, if applicable. Response and recovery strategies must also weigh into the consequence analysis. **Concern Assessment:** Identify the ramifications if the threat is miscommunicated.
Operational DM	The Operational DM can make better informed decisions based on baseline criteria through risk assessment methodologies. Tool enhancements tailored for the threat, vulnerability, consequence, and criticality for the passenger rail system assist the Operational DM with deployment analysis. Uncertainty and complexity are high, and factor into the Operational DM process. Intuitive DM may be required if an attack is imminent.
Examples:	**Threat Analysis:** Generated actionable intelligence products that support the Operational DM. Timely dissemination is critical. Intelligence/operations interface should be supported at every level of decision making. Agencies include FBI-JIC, NYPD-RIC, NJSP-ROIC. **Vulnerability Assessments (VA):** Current documentation identifying vulnerabilities to the rail transportation sector for NY/NJ. Information should enable Operational DM to make decisions based on the most vulnerable and accessible entry points. Such a large system makes this difficult to achieve. **Consequence Analysis CA**: Looks at commuter volume on given railways and the highest risk based on loss of life and the cascading impact to other infrastructure. Appropriate response measures are identified through assessment. **Concern Assessment:** Operational deployments such as the NYPD Operation Atlas, NJSP Target Hardening Response Emergency Activation Teams (THREAT) that are recognized by the public and may reduce public risk perception.
Tactical DM	The Tactical DM relies on the risk appraisal for identifying adversarial capabilities. Intent and capability will factor into the Tactical DM approach. The risk assessment should be tailored for the Tactical DM to support the best informed decisions in order to prevent and respond if an attack is executed. Uncertainty and complexity factor heavily into the Tactical DM, who is operating within the target environment and may rely on Intuitive DM skills, if need be.
Examples:	**Threat Analysis:** Generated actionable intelligence products that can support the Tactical DM. Timely dissemination is critical. Intelligence operations interface should be supported at every level of decision making, including FBI-JIC, NYPD-RIC, NJSP-ROIC. The focus is on intent and capability, and the type of explosives and delivery system (remote detonation contained within package, suicide attack) that might be used. **Vulnerability Assessments (VA):** Current documentation identifying vulnerabilities to the rail transportation sector for NY/NJ. Information enables Tactical DM to deploy detection and prevention measures at the most vital nodes. These measures may include passenger bag screening or explosive detection K9 teams. **Consequence Analysis CA**: Assess response procedures to ensure adequate life-saving measures. Entities include the NYPD, Fire Department of New York (FDNY), PAPD, NJSP, and the Northern NJ first responders.



Prioritization

- Alternatives Evaluation
- Prioritize Assets, Systems, Networks, and Functions based on Risk Assessment

Tolerability Acceptability & Judgment

- Risk Characterization
- Risk Evaluation

The Prioritization and Tolerability Acceptability and Judgment Components are placed at the lower half of the Assessment Sphere for this framework so the decision maker can take into account all relevant assessment information that is generated through the Pre-Assessment, Security Goals and Objectives, and Risk Appraisal Components. This is integral to the process prior to risk characterization and evaluation, which is aimed at judging a risk's acceptability and/or tolerability. The threat to the passenger rail system is a risk that does not translate well as being an acceptable risk. The decision maker can take into account alternative solutions based on further intelligence.

Prioritization / Tolerability Acceptability & Judgment	
Strategic DM	The Strategic DM ensures prioritization of all relevant assets, and that those involved in prevention, protection, and response understand the implementation strategies and monitoring elements. Risk assessment methodologies are re-evaluated.
Examples:	**Alternatives Evaluation:** An increased level of actionable intelligence necessitates a strategic change in the course of action. Regional law enforcement entities may redeploy based on that intelligence. Intuitive DM may be required. Responsible entities include FBI-JIC, NYPD-RIC, NJSP-ROIC. **Tolerability Acceptability Judgment:** Risk has been characterized as being unacceptable. All precautions will be carried out to prevent an attack.
Operational DM	The Operational DM ensures that operational priorities are consistent with the course of action developed by the Strategic DM, and that entities responsible for prevention, protection and response understand the implementation strategies. Clear lines of communication are established with intelligence agencies.
Examples:	**Alternatives Evaluation:** An increased level of actionable intelligence necessitates immediate operational deployment. Regional law enforcement entities may redeploy based on intelligence. Intuitive DM may be required. All regional entities are monitoring the intelligence/operations interface. **Tolerability Acceptability Judgment:** Risk has been characterized as being unacceptable. All precautions will be carried out to prevent an attack.
Tactical DM	The Tactical DM can ensure that tactical prevention and protection capabilities are available and consistent with operational deployment strategies. Entities responsible for prevention, protection and response understand the implementation strategies. Clear lines of communication are established with intelligence agencies.
Examples:	**Alternatives Evaluation:** An increased level of actionable intelligence requires immediate tactical intervention. Regional law enforcement entities may need to respond based on intelligence. There is an increased need for Intuitive DM. All regional entities are monitoring the intelligence/operations interface. **Tolerability Acceptability Judgment:** Risk has been characterized as being unacceptable. All precautions will be carried out to prevent an attack.

Risk Management

- **Management Selection**
- **Implementation**
- **Monitor Measure Effectiveness**

This component of the risk management/governance framework is assembled to ensure that all components of the risk management/governance process have been engaged by decision makers at every level. This is critical to the risk-management process, and is demonstrated through the principle decision-making tables. The strategic, operational, and tactical decision makers have all been engaged in the risk management/governance process.

The Risk Appraisal Component was the primary driver for decision making that required risk assessment methodologies and concern assessment. The Risk Management Component represents the decisions that are based on action and execution. However, this framework illustrates the connectivity among all of the components by placing communication at the core of the process. The Communication Component interconnects each of the other components and elements of this framework. This feature demonstrates that risk assessment and risk-management principles taken collectively optimize informed decision making.

The intelligence threat simulation has engaged each principle decision-making process at various levels. It is at this phase of the process that all prevention and protective measures are implemented and monitored to ensure that the best courses of action have been taken in order to drive down risk.

Risk Management	
Strategic DM	The Strategic DM can ensure that implementation by operational and tactical elements is being carried out, and intelligence monitoring as well as situational awareness is being conducted at every level. There is an increased need for intuitive decision making. Analytical processes are continuous.
Examples:	**Implementation:** Agencies that support this element include FBI-JTTF, DHS, TSA, NYPD, PAPD, NJSP, NJ Transit, Port Authority of NY/NJ. **Intelligence Monitoring & Situational Awareness:** Information sharing takes place among analytical fusion centers and the FBI-JIC, HSIN, NYPD Command and Control Center, NYPD-RIC, NJ-ROIC, NY/NJ-RISE.
Operational DM	The Operational DM can ensure that implementation by tactical elements is being carried out, and intelligence monitoring as well as situational awareness is being conducted at operational deployment locations. Analytical processes are continuous. There is an increased need for intuitive decision making.
Examples:	**Implementation:** Implementation and layered security approach throughout rail transportation system is conducted by NYPD, PAPD, NJ Transit, and NJSP. **Intelligence Monitoring & Situational Awareness:** Information sharing takes place among analytical fusion centers and FBI-JIC, HSIN, NYPD Command and Control Center, NYPD-RIC, NJ-ROIC, NY/NJ-RISE.
Tactical DM	The Tactical DM can ensure that the execution of prevention and protection activities is being carried out by tactical elements. There is an increased need for intuitive decision making. Analytical processes are continuous.
Examples:	**Implementation:** Prevention and protection measures are implemented, such as random bag searches, explosive trace detection elements, and container screening. High law enforcement presence, including NYPD Operation Atlas and NJSP Target Hardening Response Emergency Activation Teams (THREAT). **Intelligence Monitoring & Situational Awareness:** Information sharing takes place among analytical fusion centers and the FBI-JIC, HSIN, NYPD Command and Control Center, NYPD-RIC, NJ-ROIC, NY/NJ-RISE. All intelligence dissemination needs to be timely and accurate.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. RESEARCH IMPLICATIONS AND FINDINGS

1. Research Overview

This study explored the application of a risk management framework to improve the process of making decisions. It analyzed the complexity and uncertainty apparent when risk-informed decision making is required of our homeland security practitioners. The principles of decision making were integrated with each of the risk management frameworks developed by the Department of Homeland Security *(Contained in the National Infrastructure Plan — NIPP)*, the Government Accountability Office (GAO), and the International Risk Governance Council (IRGC). Based on this analysis, an assessment was made regarding whether the frameworks provide a logical set of actions that a decision maker could follow. The commonalities and core attributes were then extracted from each framework that appeared to be the most effective at addressing current risk assessment shortcomings, and was integrated into a risk management/governance framework.

This study also explored the utility of conducting a risk and threat analysis for a particular problem space found within the homeland security domain — the passenger rail transportation sector. From this analysis, the study developed a hypothetical scenario and intelligence simulation that targeted the passenger rail transportation system for New York and New Jersey. To evaluate its utility, the integrative risk management/governance framework was applied to this threat-based scenario.

2. Benefits of a Risk Management Framework for Homeland Security Decision Making

A comprehensive risk management framework can assist state and local leaders with homeland security decision making. Each of the currently available risk management frameworks can assist the decision maker with resource allocation and situational, course-of-action decisions. No single framework, however, is perfect or perfectly applicable to homeland security, mainly because of the uncertainty and complex nature of terrorism. This leaves the decision maker with a series of challenges, the most pressing of which is to manage risk in an ever-evolving arena of homeland security.

The integrated risk management/governance framework was developed to integrate the core components and elements from each of the existing frameworks. The risk management/governance process was meant to reveal the applicability of decision making throughout the risk process, combining both risk assessment and risk management principles. Essential to the risk management/governance structure was identifying the need to specify tools and proven methodologies that are tailored to a specific problem or issue.

The application of the risk management/governance framework to the passenger rail threat for New York and New Jersey revealed that strategic, operational, and tactical decision making occurs throughout the assessment process. The assessment and management spheres of risk based decision making provide the components and elements to guide the decision maker. Communication was central to the core process. Among decision makers who are engaging in risk assessment and risk management, communication can prove to be critical if, in fact, threat is introduced into an otherwise stable environment.

The qualitative analysis conducted for the passenger rail transportation sector revealed that commonalities were evident for each attack methodology. Terrorist tactics were consistent with targeting times, explosive composition, and organizational and cell structures. Due to the difficulty of applying quantitative measures as a methodology to determine threat, this qualitative analysis provided an accurate platform for the threat scenario.

3. Challenges with Risk Management Frameworks for Homeland Security Decision Making

Evident in the NIPP framework was the consistency of supporting each phase of the process with core elements and procedures that can support the decision maker.

Sector-specific agencies need to tailor their risk-management processes with guidance and direction that is relevant to a particular phase. The framework provides the structure, but decision makers should be responsible for implementing the principal features. Another challenge is ensuring that decision makers at every level of an organization are engaged in the risk-management process. Although the *strategic* decision makers developed goals/objectives and a course of action, the analysis revealed that it was the *operational* and *tactical* decision makers who carried out the action and execution. Organizational decision makers at every level should be educated in the value and utility of a risk management framework. This may guide decision makers who are required to make decisions over long duration periods, or implement immediate action.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

1. Risk Governance Framework Enhancement

The risk management/governance framework combined risk management and risk assessment under the overarching umbrella of risk governance. Both risk assessment and management principles were integrated within a core process. This process is by no means exhaustive, and it may need refinements if it is to further enhance decision making. Risk governance principles outlined in the IRGC framework are inclusive of both risk management and assessment, and they may have an application for future risk-process studies.

2. Risk and Decision Making

Principles of decision making were explored and integrated within the risk management process. Further research — incorporating decision-making principles with processes associated with managing risk — is conducive, and can support homeland security leaders. The uncertainty and complexity of managing risk requires homeland security leaders to apply adequate decision-making skills within the ever-changing landscape of homeland security.

The homeland security domain is riddled with wicked problems, uncertainty, and complex issues. Managing homeland security risk is a daunting task. If decision makers are to make the best-informed decisions, they will need to use the most appropriate tools and methodologies. Through this research, an integrative risk management/governance framework emerged. This framework may be applied by homeland security leaders who are responsible for managing risk resources; it has the potential to optimize risk reduction across various sectors. Furthermore, the utility of this framework may enhance decision making within the vast, dense problem space associated with homeland security risk.

LIST OF REFERENCES

ABC News website. "Police Investigate New York Subway Terror Threat," October 6, 2005. http://abcnews.go.com/US/story?id=1190231 [Accessed on December 27, 2007].

Bay, Austin. "Real Clear Politics: The Mumbai Terrorist Attack," July 12, 2006. http://www.realclearpolitics.com/articles/2006/07/the_mumbai_terrorist_attack.html (Accessed on October 31, 2007).

Bernstein, Peter L. *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley & Sons, 1996.

Brinkley, Joel. "F.B.I. Issues a Terror Warning, Citing Possible Threat to Trains," *New York Times*, October 25, 2002.

Bongar, Bruce, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge, Philip G. Zimbardo. *Psychology of Terrorism*. Oxford, New York: Oxford University Press, 2007.

Bush, George. *National Strategy for Homeland Security*. Washington, DC: The White House, 2007.

Bushey, David A., and Michael J. Forsyth. "The Recognition-Primed Decision Model: An Alternative to the MDMP for GWOT," *FA Journal* (January/February 2006), Military Module, 11.

Chertoff, Michael. Testimony by Secretary Michael Chertoff before the Homeland Security Subcommittee of the Senate Appropriations Committee. April 20, 2005. http://www.dhs.gov/xnews/testimony/testimony_0035.shtm. [Accessed November 1, 2006].

———. U.S. Department of Homeland Security Second Stage Review, Speech was conducted at the Ronald Regan Building, Washington, DC, July 13, 2005. http://www.dhs.gov/xnews/speeches/speech_0255.shtm. [Accessed February 5, 2007].

Congressional Research Service. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Washington, DC: Congressional Research Service, September 2, 2004.

———. *Critical Infrastructure: The National Asset Database*. Washington, DC: Congressional Research Service, September 14, 2006, Summary.

———. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences.* Washington, DC: Congressional Research Service, January 19, 2007.

———. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress.* Washington, DC: Congressional Research Service, February 2, 2007.

Conklin, Jeff. "Wicked Problems and Social Complexity" (2006), http://cognexus.org/wpf/wickedproblems.pdf [Accessed February 27, 2008].

Democratic Staff of the Committee on Homeland Security. *Detour Ahead: Critical Vulnerabilities in America's Rail and Mass Transit Security Programs.* Congressional Report prepared by the Democratic Staff of the Committee on Homeland Security, June 2006.

Ethics Resource Center, Plus: The Decision Making Process. www.ethics.org/resources/decision-making-process. [Accessed on March 3, 2008].

"Global Terrorism Analysis." Jamestown Foundation web site http://www.jamestown.org/terrorism/search.php [Accessed on October 31, 2007].

Government Accountability Office. *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*. Washington, DC: United States Government Printing Office, GAO-02-208T. October 31, 2001.

———. *Homeland Security: Applying Risk Management Principles to Guide Federal Investments.* Washington, D.C.: United States Government Printing Office, GAO-07-386T. February 7, 2007.

———. *Rail Security – Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain.* Washington, DC: Government Accountability Office, March 23, 2004, Appendix I.

———. *Risk Management – Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* Washington, D.C.: Government Accountability Office, December 2005.

———. *Transportation Security – Systematic Planning Needed to Optimize Resources.* Washington, DC: Government Accountability Office, February 15, 2005.

Gyllensporre, Dennis T. "Decision Navigation: Coping with 21st-Century Challenges in Tactical Decision Making," *Military Review* (September/October 2003), 26.

Haimes, Yacov Y. *Risk Modeling, Assessment, and Management.* Hoboken, New Jersey: John Wiley & Sons Inc., 2004.

Hawley, Kip. *Implementing Recommendations of the 9/11 Commission Act of 2007,* testimony before the U.S. Senate Committee, http://www.tsa.gov/press/speeches/101607_hawley.shtm [Accessed on October 24, 2007].

Hoffman, Bruce. *"Inside Terrorism,"* London: Orion and New York: Columbia University Press, 1998.

———. *"Inside Terrorism: Revised and Expanded Edition,"* New York: Columbia University Press, 2006.

Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, Presented to Parliament by the Prime Minister by Command of Her Majesty, May, 2006.

Jenkin, Clinton M. "Risk Perception and Terrorism: Applying the Psychometric Paradigm," *Homeland Security Affairs* II, no. 2 (July 2006), 1.

Jopek, Edward J., and Kerry L. Thomas, "Security Risk Management: Implementing a National Framework for Success in the Post 9/11 World," Appeared in a Monograph from the George Mason University School of Law's entitled, "Critical Infrastructure Protection: Elements of Risk" (December 2007), 1.

Kaufman, David J. Presentation on "Planning for Homeland Security," Director for Preparedness Policy, Planning & Analysis, Department of Homeland Security, Naval Postgraduate School, Monterey, CA, (October 10-11, 2007).

Klein, Gary. A. *Sources of Power: How People Make Decisions*. Cambridge, Mass: M.I.T. Press. 1998.

Lennart Sjoberg, Bjorg-Elin Moen, Torbjorn Rundmo. *Explaining Risk Perception: An Evaluation of the Psychometric Paradigm in Risk Perception Research,* Trondheim, Norway: Norwegian University of Science and Technology, 2004.

London Assembly, "Report of the 7 July Review Committee," Greater London Authority, June 2006, 12.

Metro Briefing New York, Manhattan: *"Man Gets Five Years In Plot To Bomb Subway," New York Times*, March 3, 2007.

Metropolitan Transit Authority web site http://www.mta.info/ [Accessed on November 6, 2007].

Mintzberg, Henry, and James B. Quinn. *The Strategy Process: Concepts and Contexts.* Englewood Cliffs, New Jersey: Prentice Hall, 1992.

MIPT Terrorism Knowledge Base web site http://www.tkb.org/Incident.jsp?incID=17994 [Accessed October 31, 2007].

MIPT Terrorism: "What's Coming the Mutating Threat," *Senior Fellows Report*, 2007, Brian M. Jenkins, Martha Crenshaw, Alex P. Schmid, Leonard Weinberg, Boaz Ganor, Gustavo Gorriti, Rohan Gunaratna, 20.

Moghaddam, Fathali M. *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy*. Westport, Connecticut: Praeger Security International, 2006. 123-124.

New Jersey Transit web site http://www.njtransit.com/tm/tm [Accessed on November 6, 2007].

News Scientist Tech: Explosives Linked to London Bombings Identified, July 15, 2005. Web site http://technology.newscientist.com/article/dn7682 [Accessed on November 3, 2007].

Paczkowski, John P. "Risk Management as Strategic Change in National Homeland Security Policy," Naval Postgraduate School Thesis, September 2007, 14.

Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terrorism*. New York: Random House, 2005.

Rashbaum, William K., and William Newman, "PATH Tunnels Seen as Fragile in Bomb Attack," *New York Times*, December 22, 2006.

Ross, Karol G., Gary A. Klein, Peter Thunholm, John F. Schmitt and Holly Baxter, "The Recognition-Primed Decision Model," *Military Review* (July/August 2004), Military Module, 6.

Ross, Robert G. "Risk and Decision Making in Homeland Security." *Office of Comparative Studies, Department of Homeland Security Science and Technology Directorate* (July 31, 2006): 1-23.

Renn, Ortwin. "Risk Governance Towards and Integrative Approach." International Risk Governance Council, Geneva (September 2005): 1-156.

Renn, Ortwin and Katherine D. Walker. *Global Risk Governance: Concept and Practice Using the IRGC Framework*. Berlin, Germany: Springer Publishing, 2008).

Shapira, Zur. *Risk Taking: A Managerial Perspective*. New York: Russell Sage Foundation, 1994.

Slovic, Paul. *The Perception of Risk*. London: Earthscan Publications Ltd, 2000.

Slovic, Paul, and Elke Weber, "Perception of Risk Posed by Extreme Events," Paper presented at the conference Risk Management Strategies in an Uncertain World, Palisades, New York, April 12-13, 2002, 12.

Suskind, Ron. *The One Percent Doctrine: Deep Inside America's Pursuit of its Enemies Since 9/11*, New York, NY: Simon & Schuster, 2006.

"Target Capabilities List: A companion to the National Preparedness Goal, Department of Homeland Security." (August 2006), vi, http://www.emaponline.org/?294 [Accessed on February 20, 2008].

The 9/11 Commission. *The 9/11 Commission Report: Final Report of The National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Co, 2004.

Transportation Security Administration. *Risk Management.* http://www.tsa.gov/approach/risk/index.shtm [Accessed October 18, 2007].

The Society for Risk Analysis, http://www.sra.org/events_2007_meeting.php [Accessed December 18, 2007].

United States Coast Guard's Glossary of Risk Terms, http://www.uscg.mil/hq/gm/risk/glossary.html [Accessed on March 18, 2008].

United States Department of the Army. "Army Planning and Orders Production." *Field Manual 5-0*: Washington, DC (January 20, 2005): 1-328.

United States Department of Homeland Security. *National Infrastructure Protection Plan*. 2006. Washington, DC: U.S. Department of Homeland Security.

———. *National Preparedness Goal*. December 2005. Washington, DC: U.S. Department of Homeland Security.

———. *Homeland Security Grant Program: FY 2006 Fact Sheet Series, Overview, Peer Review Process, Risk Analysis, Effectiveness Analysis, Allocation Methodology.* http://www.ojp.usdoj.gov/odp/newsreleases. [Accessed October 2006].

United States Department of Justice, *Assessing and Managing the Terrorism Threat,* September 2005.

United States Government Accountability Office. *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*. Washington, DC: United States Government Printing Office, GAO-02-208T. October 31, 2001.

———. *Homeland Security: Applying Risk Management Principles to Guide Federal Investments.* Washington, DC: United States Government Printing Office, GAO-07-386T. February 7, 2007.

United States Nuclear Regulatory Commission: Full text Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html [Accessed January 28, 2008].

Willis, Henry, Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby. *Estimating Terrorism Risk*. Santa Monica, CA: RAND Center for Risk Management Policy, 2005.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Colonel Joseph Fuentes
   New Jersey State Police
   West Trenton, New Jersey

4. LTC Thomas Gilbert
   New Jersey State Police
   West Trenton, New Jersey

5. LTC Richard Arroyo
   New Jersey State Police
   West Trenton, New Jersey